

Risikomanagement

Yannic Döll, Lennart Dümke, Niklas Herz, Martin Arendt, Ken Madlehn

Zuverlässigkeit und Sicherheit – WiSe 2019/2020

Prof. Dr. rer. nat. Christoph Thiel

Team

- | | |
|-----------------|---------|
| • Yannic Döll | 1157815 |
| • Lennart Dümke | 1151181 |
| • Niklas Herz | 1151318 |
| • Martin Arendt | 1151251 |
| • Ken Madlehn | 1181333 |

Themen

- Risiken
- Risikomanagement
 - Risikoidentifikation
 - Risikoanalyse/ -bewertung
 - Risikobewältigung
 - Risikoüberwachung
- Risikokommunikation

Was sind Risiken

- Sachverhalt in der Zukunft
- Ungewisser Ausgang
- Negative Auswirkung
- Kombination aus Bedrohung und Sicherheitslücke

Arten von Risiken

- Marktrisiken
- Betriebsrisiken
- Finanzrisiken
- Umweltrisiken
- Sonstige Risiken

Risikomanagement

- Aktivitäten im Umgang mit Risiken
- Ziel: Risiken positiv beeinflussen
- Kosten-Nutzen-Analyse
 - Aspekte: Wirkung, Eintrittswahrscheinlichkeit
 - Voraussetzung: Risiken identifizieren und überwachen

ISO 31000

- Beschäftigt sich mit dem Umgang mit Risiken in einer Organisation
- Prinzipien
 - Risikomanagement als Führungsaufgabe
 - Top-Down-Ansatz
 - Allgemein gehalten

ISO 31000 – Plan, Do, Check, Act

- Plan

Auftrag und Verpflichtungen der Risikopolitik

- Do

Risikomanagementprozess

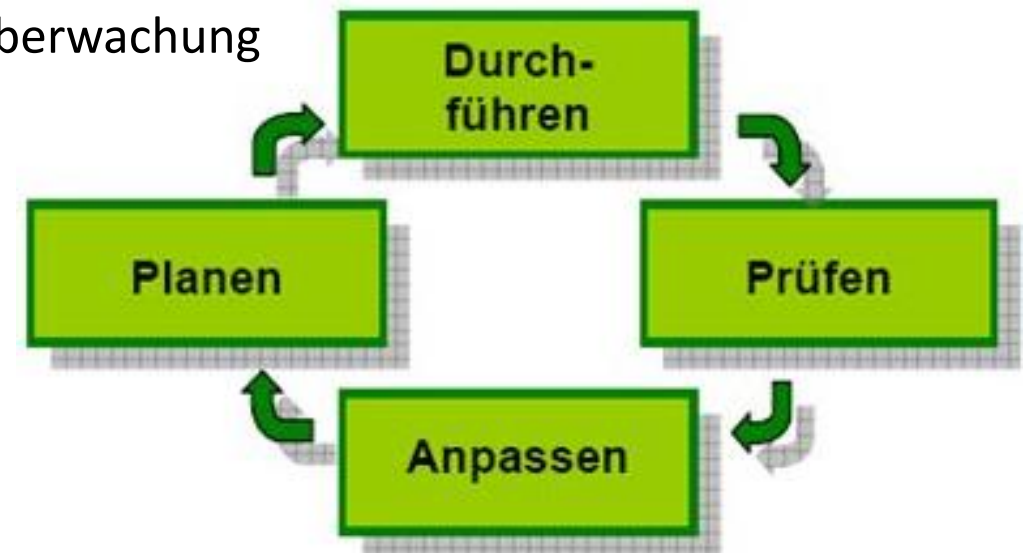
→ Identifikation, Analyse, Bewertung, Bewältigung, Überwachung

- Check

Risikobewältigungsstrategien und Planabweichungen überprüfen

- Act

Anpassungen vornehmen



ISO 31000 - Intentionen

- Risikomanagement an bestehende Managementsysteme anbinden
- Risikomanagementprozess optimieren
- Abstand von der reinen Gesetzesbefolgung nehmen
- Übergang von passiver zu aktiver Denkweise

ISO 31000 - Risikobeauftragter

- Ansprechpartner für Mitarbeiter und Führungskräfte
- Zuständig für Risikoberichterstattung
- Berichtet regelmäßig dem Vorstand der Geschäftsführung
- Risikosituation und Handlungsbedarf darstellen

Gesetz zur Kontrolle und Transparenz (KonTraG)

- 1998 in Kraft getreten
- Ziele
 - Corporate Governance weiterentwickeln
 - Haftung von Vorstand, Aufsichtsrat, Wirtschaftsprüfer
 - Risikofrüherkennungssysteme sind Pflicht
 - Zuständigkeit von Vorstand und Aufsichtsrat
 - Prüfung durch Abschlussprüfer
 - Aussagen über Risiken im Lagebericht

Risiken identifizieren

- Risikogruppen
- Risiken identifizieren

Risiken identifizieren

- Können zum Ausfallen von Geschäftsprozessen führen
- Können Risikogruppen zugeordnet werden

Risiken identifizieren: Risikogruppen

- Interne Risiken
 - Entstehen aus Unternehmenstätigkeit
 - Ausfall von Maschinen wegen Fehlbedienung durch Mitarbeiter
- Externe Risiken
 - Wirken von außen auf eine Institution
 - Produktionsprozesse werden durch Umweltauflagen beeinflusst

Risiken identifizieren: Risikogruppen

- Direkt wirkende Risiken
 - Führen sofort zum Ausfall von Geschäftsprozessen
 - Ausfall Maschine = Produktionsunterbrechung
- Indirekt wirkende Risiken
 - Führen nicht direkt zum Ausfall von Geschäftsprozessen
 - Wartungsintervalle von Maschinen werden vernachlässigt

Risiken identifizieren: Risikogruppen

- Durch Institution beeinflussbare Risiken
 - Können selbst bestimmt werden
 - Wartungsintervalle von Maschinen
- Durch Institution nicht beeinflussbare Risiken
 - Wenig Spielraum zur Beeinflussung
 - Gesetzliche Auflagen

Risiken identifizieren: Risikogruppen

- Sonstige Risiken
 - Höhere Gewalt
 - Technisches Versagen
 - Vorsätzliche Handlungen

Risiken identifizieren

1. Abgrenzung des Analysebereiches
2. Identifikation der bedrohten Objekte
3. Identifizieren der Risiken
4. Bewertung der Risiken

Risiken identifizieren

1. Abgrenzung des Analysebereiches

- Bereich spezifizieren
 - Hardware Servercluster
- Prioritäten festlegen
 - Nur produktive Server betrachten

Risiken identifizieren

2. Identifikation der bedrohten Objekte

- Erfassung aller Assets, die im Analysebereich liegen
 - Versorgungsspannungen Netzteile: 230V, 3.3V, 5V, 12V
 - Versorgungsspannung Batterie: 3V
 - Temperaturen: RAM, HDD, CPU, Chipsatz, Peripherie
 - Lüfter: Drehzahl
 - Gehäusesensor

Risiken identifizieren

3. Identifizieren der Risiken

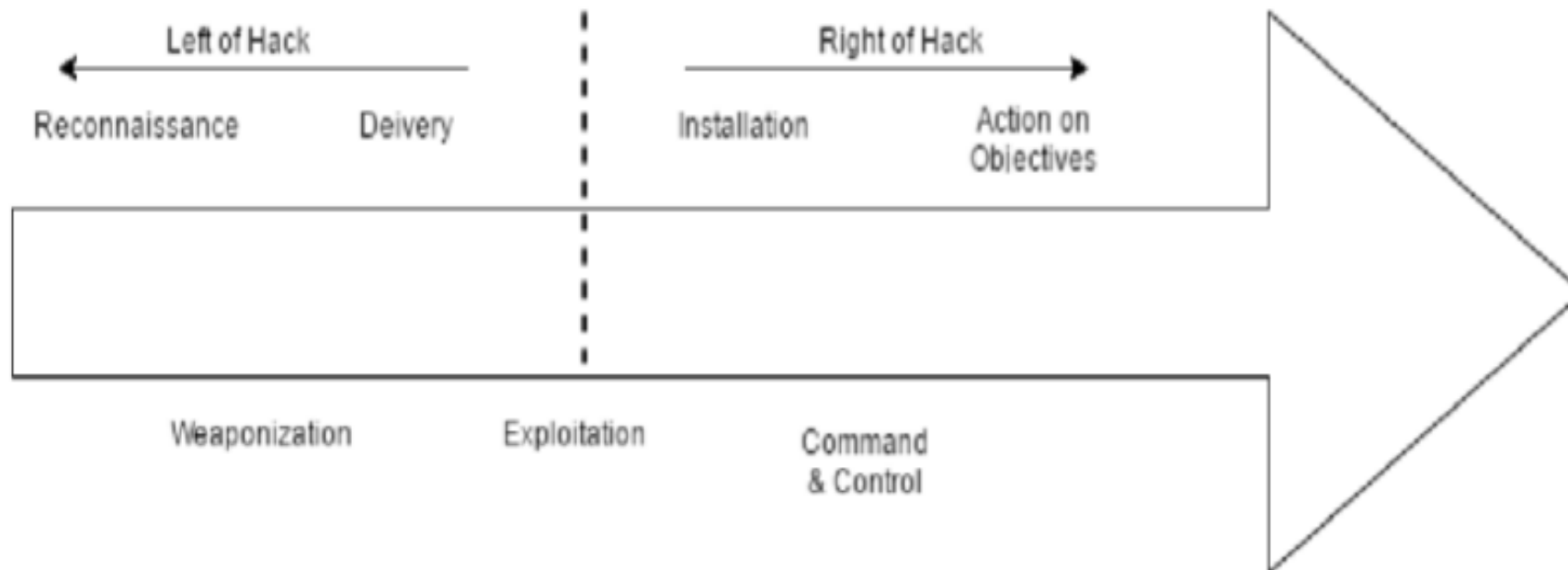
- Unregelmäßigkeiten in der Stromversorgung
 - Netzteile: Ausfall oder Spannungsschwankungen
 - Batterie: Kapazität zu niedrig oder nicht vorhanden
- Temperaturüberschreitungen
 - Von RAM, HDD, CPU, Chipsatz oder Peripherie
 - Durch Überlastung oder Ausfall von Lüfter(n)
- Ausfall Server, Rack oder Rechenzentrum

Angreifer-Modelle

Mithilfe von Angreifer-Modellen können Schwachstellen im System analysiert bzw. gefunden werden und Sicherheitsmaßnahmen getroffen werden

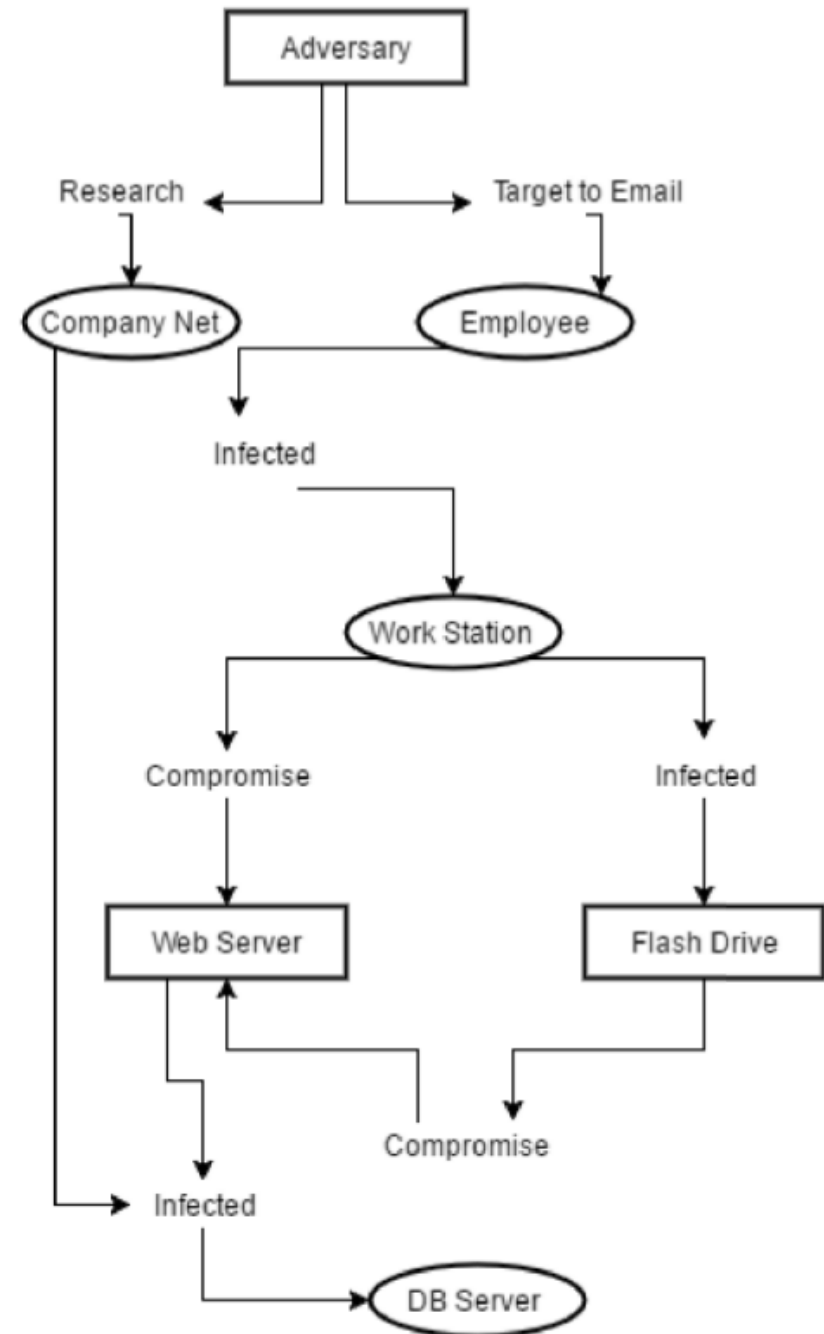
Angreifer-Modelle

Kill-Chain: Dieses Modell definiert verschiedene Stufen eines Angriffes, sowie einen kritischen Punkt (Exploitation), ab dem der Angriff um einiges schwieriger aufzuhalten ist. Mit dem Modell können Prioritäten in Bezug auf Sicherheitsmaßnahmen festgelegt werden.



Angreifer-Modelle

Attack-Graph: Mit diesem Modell können unterschiedliche Wege für ein geplantes Angriffsziel systematisch untersucht werden. Im Unterschied zum Bedrohungsbaum sind hier auch die Kanten beschriftet und Zwischenstationen aufgelistet, deswegen ist die Analyse „technischer“ und detaillierter.



Risikoanalyse und Bewertung

- BSI: Meistens reichen Standard-Sicherheitsmaßnahmen des IT-Grundschutzes aus
Aber: Falls Sicherheitsanforderungen eines Systems über das normale Maß hinausgehen, muss eine erweiterte Risikoanalyse durchgeführt werden
- Formel: $\text{Risiko} = \text{Wahrscheinlichkeit} \times \text{Schaden}$
- Grundsätzlich nur grob abschätzbar, da die Wahrscheinlichkeit und die Auswirkung nicht exakt zu beziffern sind

Bewertung der Bedrohungen

- Vorgehen: Risikomatrix erstellen
- Je nach Komplexität verschieden viele Stufen
- BSI - Grundschatz Wahrscheinlichkeiten:
 - selten (< 1x alle 5 Jahre)
 - mittel (1x alle 1-5 Jahre)
 - häufig (1x im Jahr - 1x im Monat)
 - sehr häufig (> 1x im Monat)

Beispielhafte Risikomatrix

Stufe 5 Sehr hohe Eintrittswahrscheinlichkeit	5	10	15	20
Stufe 4 Hohe Eintrittswahrscheinlichkeit	4	8	12	16
Stufe 3 Mittlere Eintrittswahrscheinlichkeit	3	6	9	12
Stufe 2 Geringe Eintrittswahrscheinlichkeit	2	4	6	8
Stufe 1 Sehr geringe Eintrittswahrscheinlichkeit	1	2	3	4
	Stufe 1 Geringer Schaden	Stufe 2 Normaler Schaden	Stufe 3 Hoher Schaden	Stufe 4 Sehr hoher Schaden

Eintrittswahrscheinlichkeit

- Es gibt verschiedene Methoden, um diese zu bestimmen, zum Beispiel durch Abwägung des Aufwands für den Angreifer und des Nutzens für den Angreifer
- Bewertung des Nutzen für den Angreifer hängt stark von seinem Motiv ab (wirtschaftliche Interessen, Neugier, vielleicht aber auch Rache?)
→ Schwer zu beurteilen
- Bewertung des Aufwands durch Penetration Tester: Bezahlte „Hacker“, die in einem System gezielt nach Schwachstellen suchen und diese dann dem Besitzer melden

Schaden

- Unterteilung in primäre und sekundäre Schäden
- Primäre Schäden:
Produktivitätsausfall, Wiederbeschaffungs-/Wiederherstellungskosten, Personalkosten
→ Sind leicht zu beziffern
- Sekundäre Schäden:
Imageverlust, Vertrauensverlust bei Kunden und Geschäftspartnern
→ langfristige Schäden, die schwer abschätzbar sind

Risikobewertung

Unterscheidung in qualitative und quantitative Risiken

Quantitative Methoden

- Risikoabschätzung in Form eines numerischen Maßes
 - Wert der Ressourcen
 - Frequenz der Bedrohungen
 - Anfälligkeit gemessen in der Wahrscheinlichkeit eines Verlustes

Quantitative Methoden

- Vorteile:
 - Akkurateres Bild der Bedrohungen
 - Erlaubt Kostenkalkulation und begünstigt eine genaue Priorisierung der Maßnahmen
- Nachteile:
 - Ergebnis evtl. ungenau und verwirrend
 - Analyse mit quantitativen Methoden generell teurer und erfordert mehr Erfahrung und fortgeschrittene Methoden

Quantitative Methoden

Beispiel:

- ALE model (Annual Loss Expected)
- $ALE = (\text{Probability of event}) \times (\text{value of loss})$
- Summe aller prognostizierten Verluste

Qualitative Methoden

- Beschreibungen, Empfehlungen
- Qualitative Beschreibung der Vermögenswerte
- Beschreibung von Angreifer-Szenarien

Qualitative Methoden

Vorteile:

- Einschätzung der Risiken ohne größeren Aufwand, Zeit und Kosten
- Erlaubt eine einfachere Einordnung der Risiken nach Priorität

Qualitative Methoden

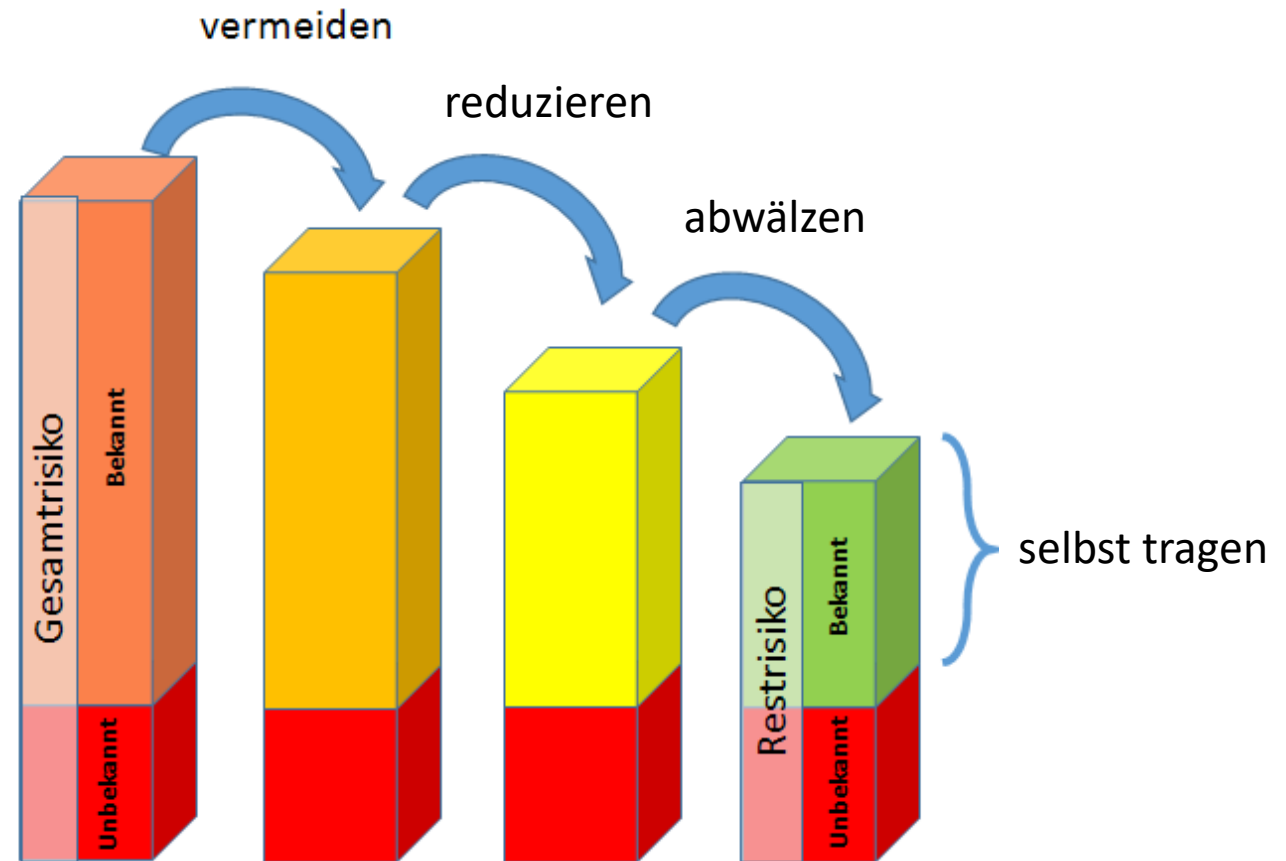
Nachteile:

- Keine Bestimmung von Wahrscheinlichkeiten möglich
- Kosten-Analyse schwieriger durchzuführen
- Resultate sind weniger akkurat und sind eher geschätzt

Risikobewältigung

Aufgaben

- Für die identifizierten Risiken eine Risikostrategie entwickeln
- Die notwendigen Handlungsmaßnahmen festlegen



Strategien:

1) Risikovermeidung

Eintreten von Risikoereignissen verhindern

- Auf Technologien verzichten
- Aus einem riskanten Projekt aussteigen

2) Risikoreduzierung

Risiko soll tolerierbar werden

- a) ... durch Verminderung der Eintrittswahrscheinlichkeit
 - Brandschutz/ Diebstahlsicherung
- b) ... durch Verminderung der Schadenshöhe
 - Sprinkleranlage



Strategien:

3) Risikotransfer/ -abwälzung

Überträgt die Risiken an Dritte

- Fremdversicherung
- Instrumente des Finanzmarktes
- Vertragsgestaltung mit Kunden und Lieferanten

4) Risikoteilung/ -streuung

Gesamtrisiko in verschiedene kleine Einzelrisiken zerteilen

- Großrechner in mehreren Containern getrennt versenden
- Breite Kundenbasis

Strategien:

5) Risikotragung

Unternehmen trägt das Risiko selbst

a) Passives Verhalten

- Risiken ignorieren (z.B. Naturkatastrophen)

b) Aktives Verhalten

Risikodeckungspotential aufbauen:

- Eigenkapital erhöhen
- Liquiditätsreserven schaffen

Risikocontrolling

- Risiken berücksichtigen während Projekt-
 - Planung
 - Steuerung
 - Kontrolle
- Verbessert Risikobewusstsein bei
 - Mitarbeitern
 - Unternehmensleitung
- Risiken werden in ein IT-System eingetragen und gepflegt

Risikoüberwachung

- Risikoindikatoren
 - Messbare Größe
 - Eintrittswahrscheinlichkeit eines Risikos
 - Werden in der Risikoüberwachung ermittelt
- Vergleichbar mit sich wiederholender Risikoidentifizierung
 - Risikoindikatoren werden aktualisiert
 - Neue Risiken werden erkannt
- Festlegung von Grenzwerten
 - Handlungsanweisungen für Risikosteuerung ableiten

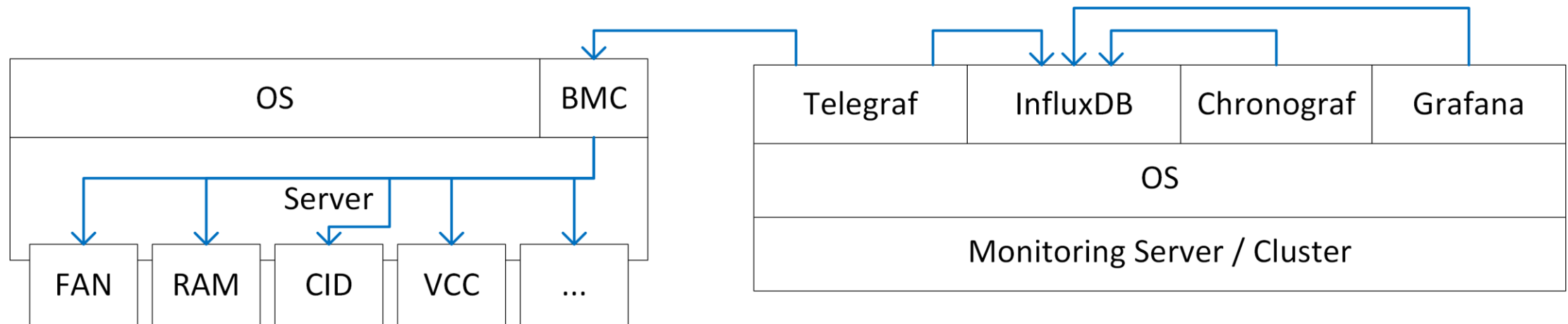
Risikoüberwachung

Im Beispiel „Hardware Servercluster“

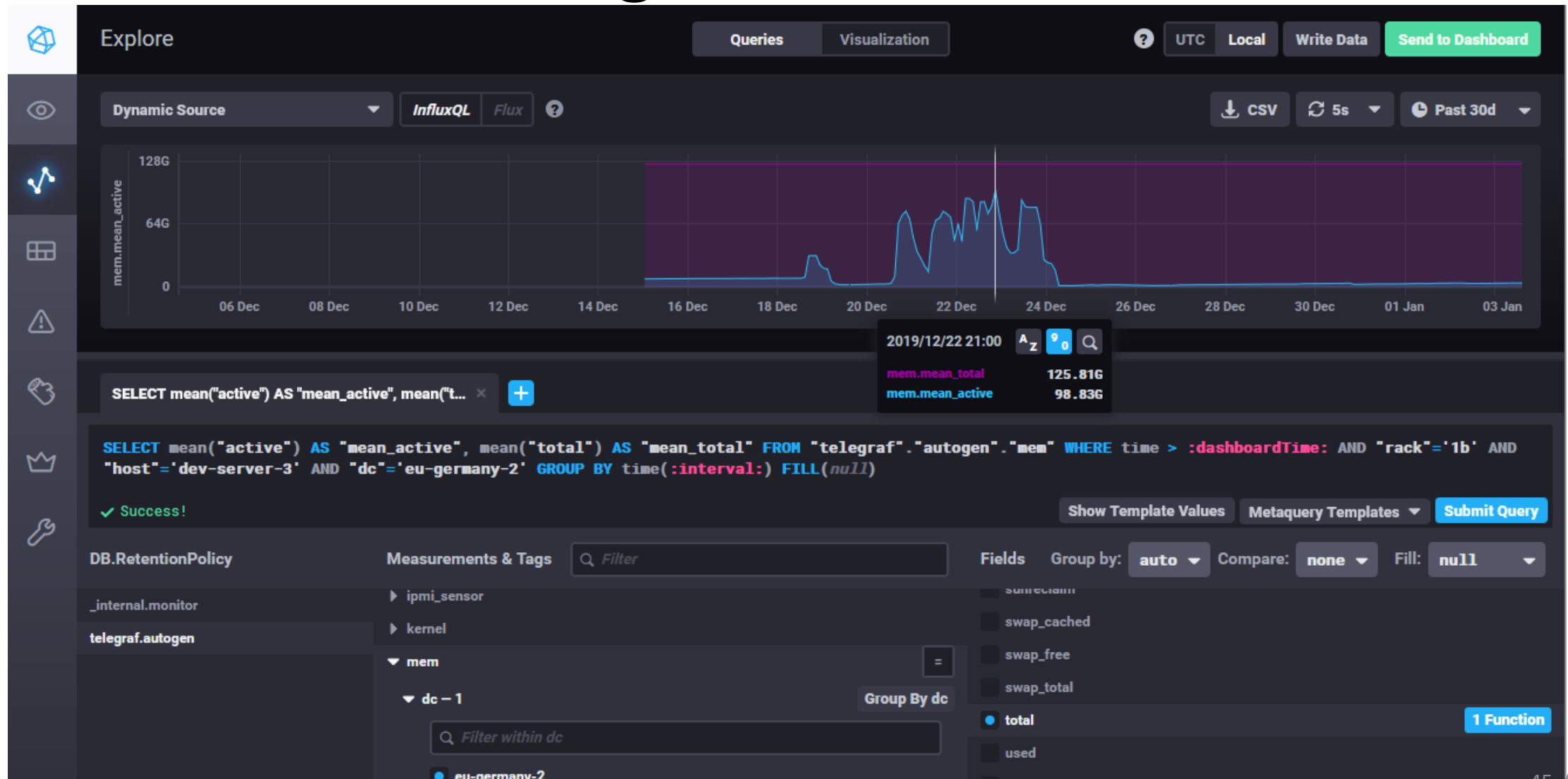
- Risiken können bereits gemessen werden
 - Temperatur, Drehzahl, Spannung
- Datenerfassung sammelt Daten, die zu keinem Risiko gehören
 - Spannung BMC, Statuscodes, CPU- u. RAM Last und Cache, etc.
 - Standort Server (Rechenzentrum, Rack, Host)
- Aus diesen Daten können neue Risiken abgeleitet werden
 - Nutzung alter Server durch deren Energiebedarf zu teuer
 - Überlastung Backbone
 - Durch Nutzung von HDD- statt U.2 Speicher nicht konkurrenzfähig

Risikoaufzeichnung

Speicherung von Risikoindikatoren aus der Risikoüberwachung



Risikoüberwachung



Risikoberichterstattung

- Aufbereitung der Daten aus der Risikoaufzeichnung
- Zeigt Veränderungen von Risiken
- Trend von Risikoindikatoren kann festgestellt werden

Risikoberichterstattung



Risikokommunikation

1) Interne Risikokommunikation

- Mitarbeiter in das Risikomanagement mit einbinden
 - ➔ Risikokultur schaffen
- Unterschiedliche Kommunikationskanäle
- Top-down Kommunikation
- Bottom-up-Kommunikation



Risikokommunikation

2) Externe Risikokommunikation

- Veröffentlichungen von Risiken:
 - ... dürfen nur durch einen Kanal erfolgen
 - ... müssen vorab von der Geschäftsleitung genehmigt werden
- Kommunikation hängt von den Informationsbedürfnissen der Stakeholder ab
- Nachhaltiges Vertrauensverhältnis mit dem Kunden aufbauen

Literaturverzeichnis

- Ibers, Tobias / Hey, Andreas: Risikomanagement, Merkur Verlag Rinteln, 2005.
- Gleißner, Werner / Romeike, Frank: Risikomanagement – Umsetzung, Werkzeuge, Risikobewertung, Rudolf Haufe Verlag, 2005.
- Stiefl, Jürgen: Risikomanagement und Existenzsicherung, Oldenbourg Wissenschaftsverlag, 2010.
- Macharzina, Klaus / Wolf, Joachim: Unternehmensführung. Das internationale Managementwissen. Konzepte – Methoden – Praxis, 8. Aufl., Gabler Verlag, 2012.
- Tiemeyer, Ernst: Handbuch IT-Projektmanagement, 2. Aufl., Carl Hanser Verlag München, 2014.
- Claudia, Eckert: IT-Sicherheit Konzepte – Verfahren – Protokolle, 4. Aufl., Oldenbourg Wissenschaftsverlag, 2006.

Literaturverzeichnis

- Meier, Alisha: Risikomanagement – so bleibst du auf alles vorbereitet! (10.10.2019), unter: <https://sevdesk.de/blog/risikomanagement/> (abgerufen am 23.12.2019)
- Schröder, Axel: Risikosteuerung im Risikomanagementprozess, unter: <https://axel-schroeder.de/risikomanagementprozess-risikosteuerung/> (abgerufen am 23.12.2019)
- Tipps zur sinnvollen Definition von Risikobewältigungsmaßnahmen (25.10.2017), unter: <https://www.3grc.de/risikomanagement/risikobewaeltigungsmassnahmen-sinnvoll-definieren-und-umsetzen/> (abgerufen am 23.12.2019)
- IT-Grundschutz, Lerneinheit 7.9: Risiken behandeln, unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_7_Risikoanalyse/Lektion_7_09/Lektion_7_09_node.html (abgerufen am 23.12.2019)
- <https://www.projektmagazin.de/glossarterm/risikoidentifikation>
- <https://www.dsin-blog.de/2014/02/10/it-risikoanalyse/>

Literaturverzeichnis

- Cyber-Attack Modeling Analysis Techniques: An Overview (August 2016), unter: https://www.researchgate.net/publication/307174392_Cyber-Attack_Modeling_Analysis_Techniques_An_Overview (abgerufen am 12.01.2020)
- Rot, Artur: IT Risk Assessment: Quantitative and Qualitative Approach (2008)
- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/4_RisikenAnalysieren/1_Risiken%20identifizieren/RisikenIdentifizieren_node.html
- <https://www.projektmagazin.de/glossarterm/risikoueberwachung>
- <https://www.projektmagazin.de/glossarterm/risikoindikator>
- <https://www.controllingportal.de/Fachinfo/Risikomanagement/Risikocontrolling.html>
- <https://www.haufe-akademie.de/blog/themen/controlling/risikomanagement/>
- <https://wirtschaftslexikon.gabler.de/definition/gesetz-zur-kontrolle-und-transparenz-im-unternehmensbereich-kontrag-52536>
- https://www.risikomanagement-wissen.de/risikomanagement/risikomanagement-einfuehrung/iso_31000/

Abbildungsverzeichnis

- <https://www.3grc.de/risikomanagement/risikobewaeltigungsmassnahmen-sinnvoll-definieren-und-umsetzen/>
- <https://www.jn-brandschutz.de/leistungen/pruefung-und-wartung-sprinkleranlage-41>
- <https://www.pixtastock.com/illustration/45199284>
- https://www.risikomanagement-wissen.de/risikomanagement/risikomanagement-einfuehrung/iso_31000/

Noch Fragen?

