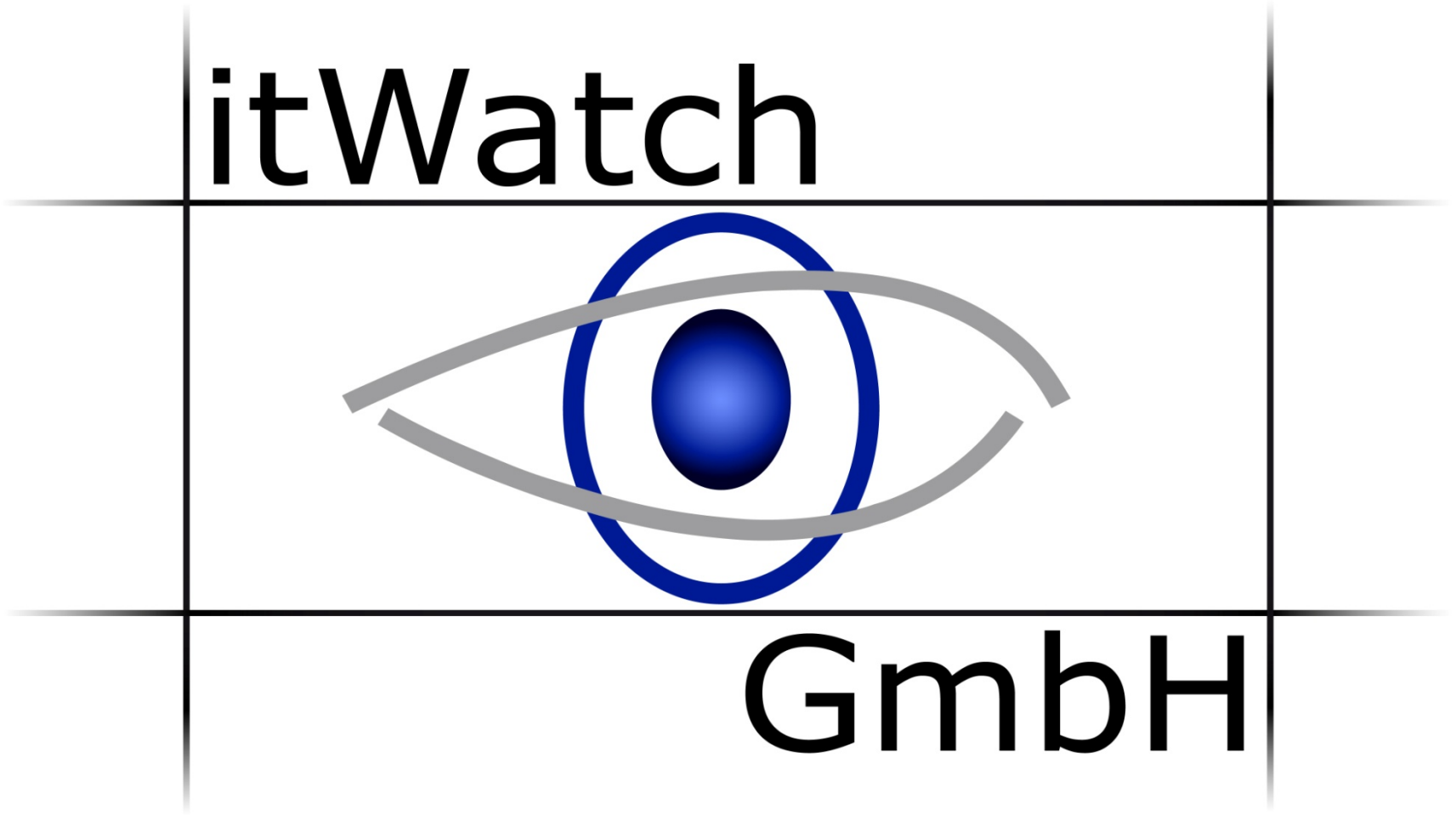
Ihre Sicherheit …
… unsere Mission



Blueprint für eine Robuste Sicherheitsarchitektur

Handlungsvorschlag für MK

Montag, den 18. Juli 2016, Unterföhring

3. Arbeitstreffen AK Security Münchner Kreis

Autor: Ramon Mörl (Geschäftsführer, itWatch)

Kurzvorstellung Ramon Mörl

- 25 Jahre Erfahrung als Berater in der IT-Sicherheit
- Leitende Tätigkeiten in Projekten für Firmen wie HP, IBM, Siemens, ICL und Bull in Belgien, Deutschland, Frankreich, Italien, Österreich, Schweiz und USA
- Als unabhängiger Evaluator und Berater der Europäischen Union vor allem im Bereich der ECMA und ISO-Standards für die IT-Sicherheit tätig
- Seit 2002 **Geschäftsführer der itWatch GmbH**

Ihre Sicherheit …
… unsere Mission

Agenda:

1. Ausgangssituation
2. **Das Problem**
3. **Das Ziel**
4. **Ausblick**

Sicherheit messen – open space

- Warum wollen wir Sicherheit messen?
- Ausrichtung an den Schutzzielen?
- Wie definieren wir Sicherheit?
- Wie wollen wir es hinterher darstellen?
- Risikobetrachtung auf Maßeinheit abbilden
- Kann man KPI‘s auf IT-Sicherheit ableiten?
- Handlungskette Audit, Pen-Test, Grundschutz, ISO 27001, ISIS 12 bis zum etablierten Schutz fortsetzen

Ausgangssituation

- Unternehmensentscheider nehmen IT-Sicherheit wie folgt wahr:
  - Technikgetrieben - nicht nutzergetrieben
  - Extrem komplex – mit widersprüchlichen Expertenmeinungen
  - Kein „hartes“ Ziel
  - Mehrwerte unklar
- Hersteller finden auf der Einkaufsseite keine IT-Sicherheitskompetenz, die den Schutzgrad „einpreisen“ kann
- Der Markt ist in großen Teilen getrieben durch Margen und Umsätze – nicht durch das eigentliche Ziel: erreichbarer Schutz
- Papier und Anweisungen schützen nicht!

<kes> Artikel - itWatch

In dem Artikel:

„Stets bemüht um Sicherheit“

Wird herausgearbeitet, dass an vielen Stellen IT-Security Know-how benötigt wird, wenn eine durchgehende gleich hohe Robustheit in einer Vertrauenskette entstehen soll:

Im Fall BW: Anforderer, Projektleiter, Planer, Beschaffer, Integrator … Administrator, Nutzer???

Bei Interesse Lesen Sie den Artikel in der <kes> 2016#2 und 2016#3-Ausgabe mit Beispielen, Fragen und Gedanken dazu, warum in Sachen Security so viel schiefgeht!

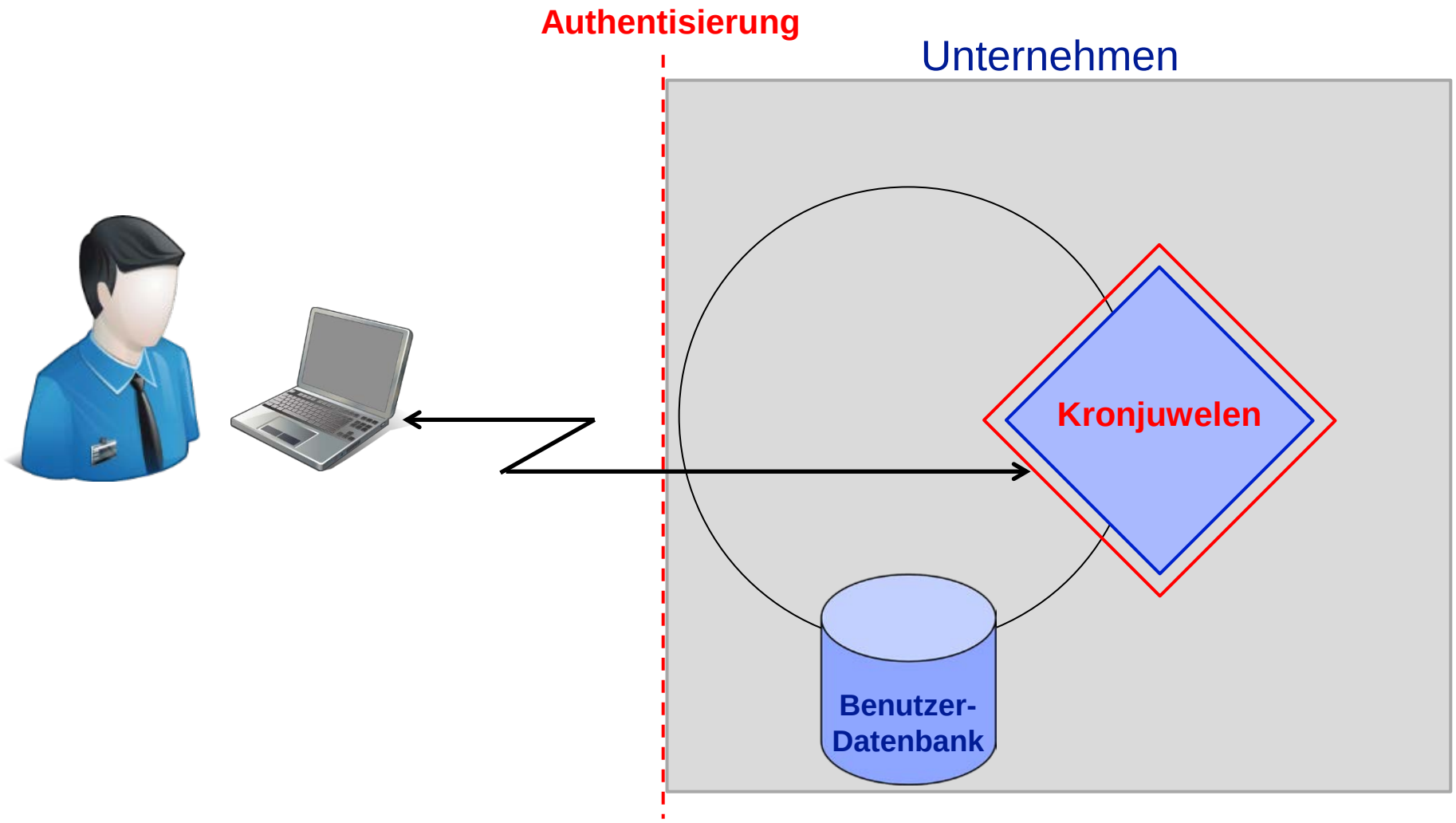
Auch online verfügbar unter:
https://www.kes.info/aktuelles/kes/stets-bemueht-um-sicherheit-1/

Ihre Sicherheit …
… unsere Mission

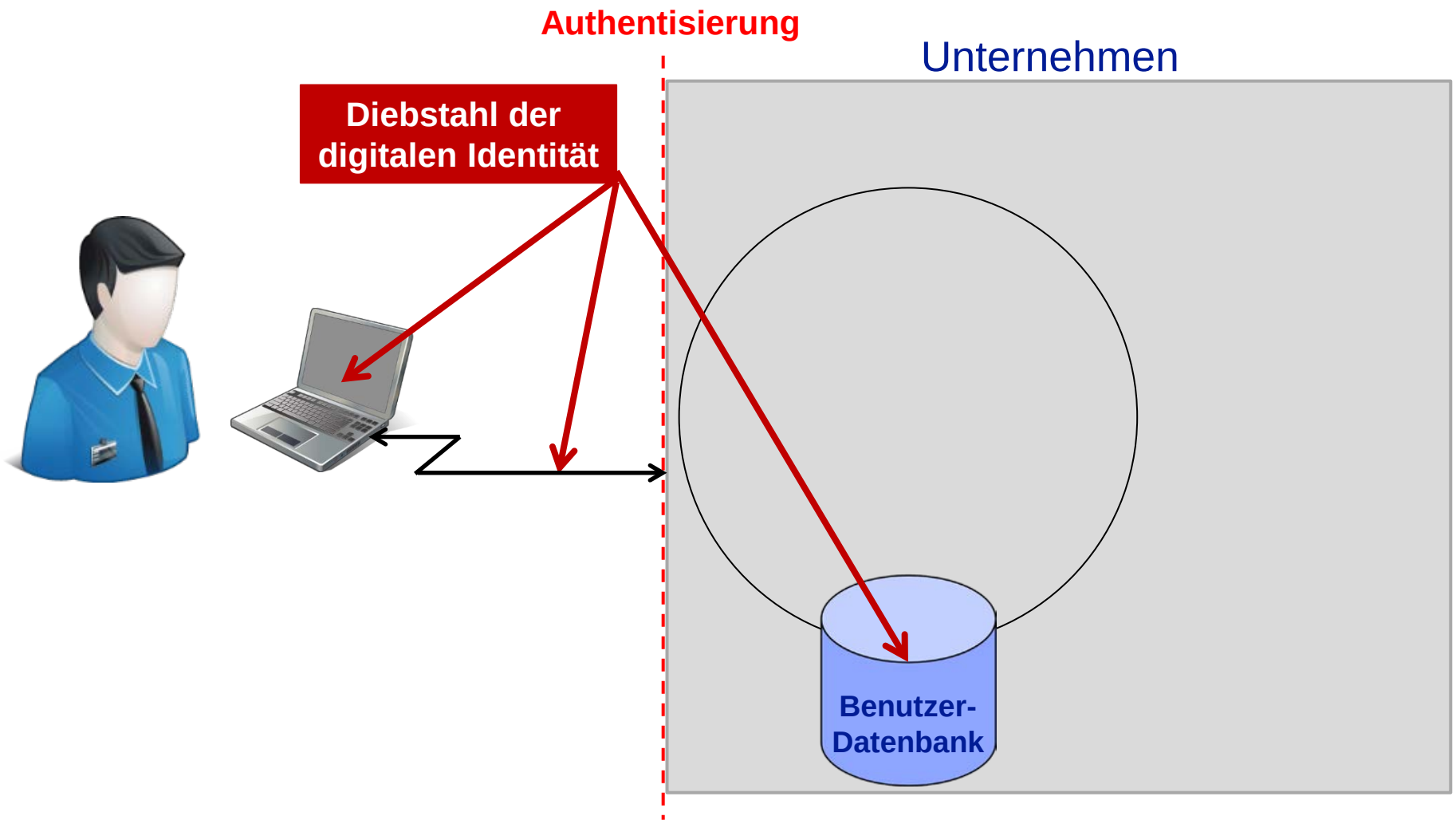
Agenda:

1. **Ausgangssituation**
2. **Das Problem**
3. **Das Ziel**
4. **Ausblick**

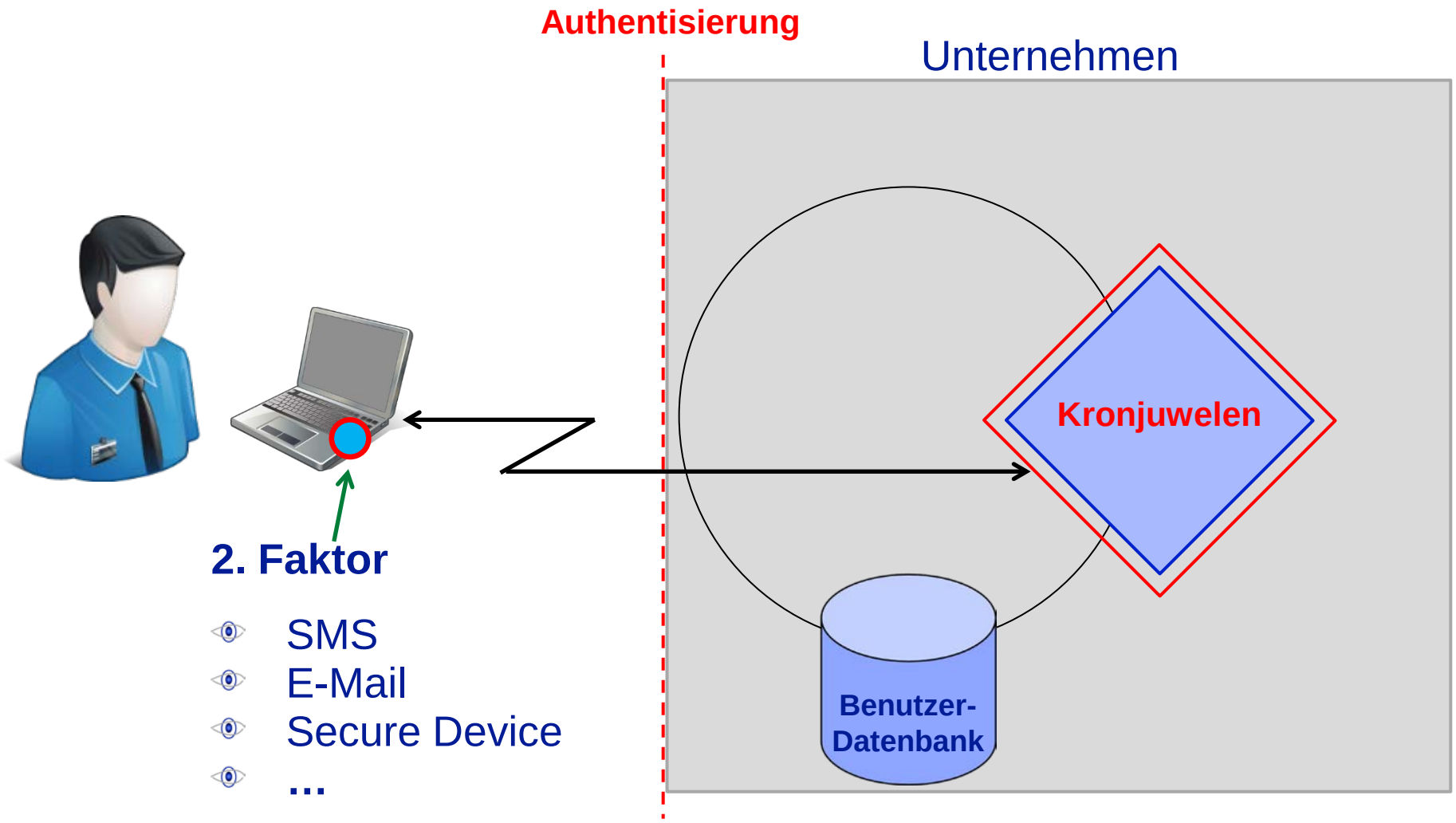
Zugriff auf Kronjuwelen



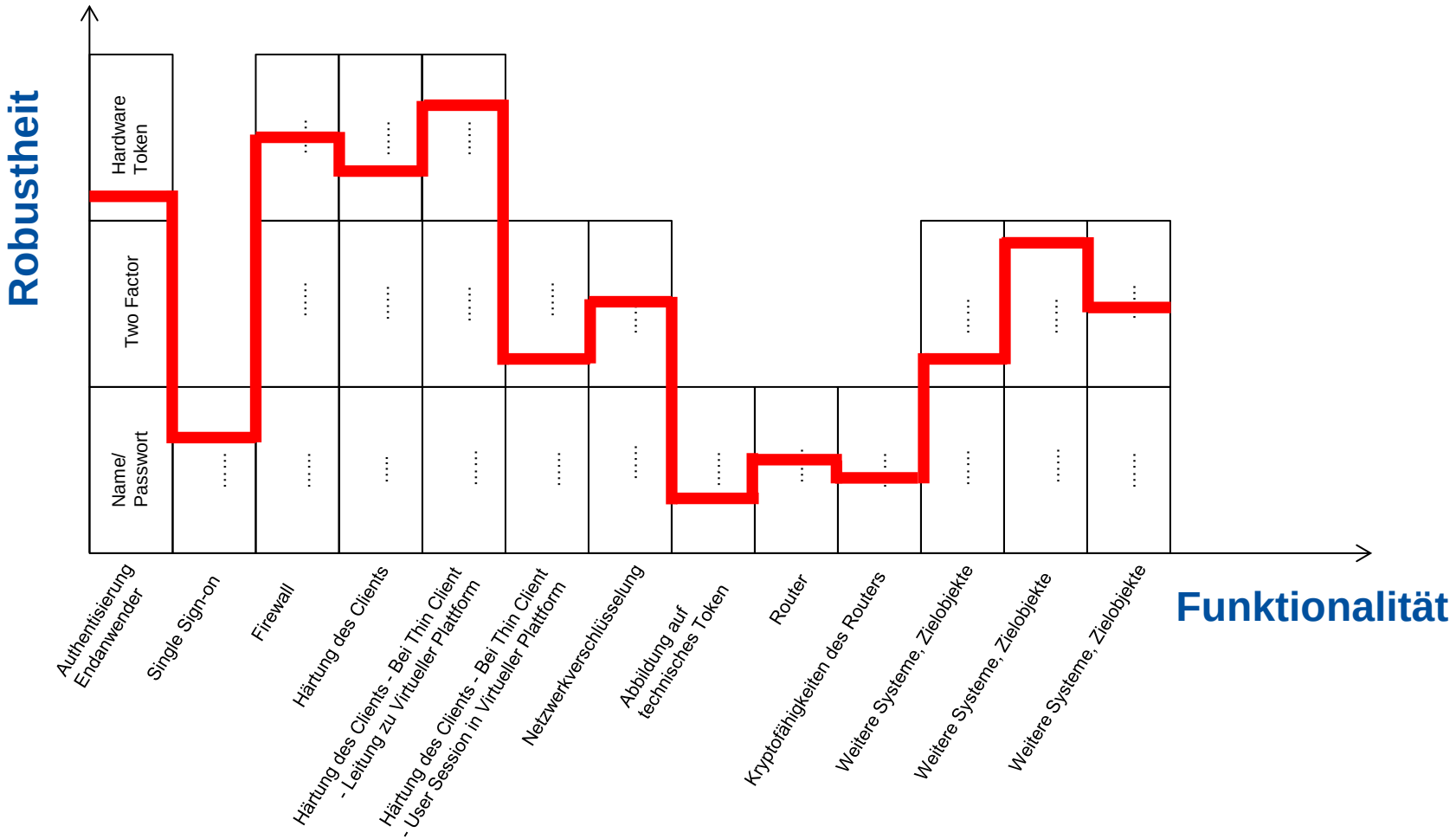
Teilproblem Authentisierung



Sinnhafte Lösung?

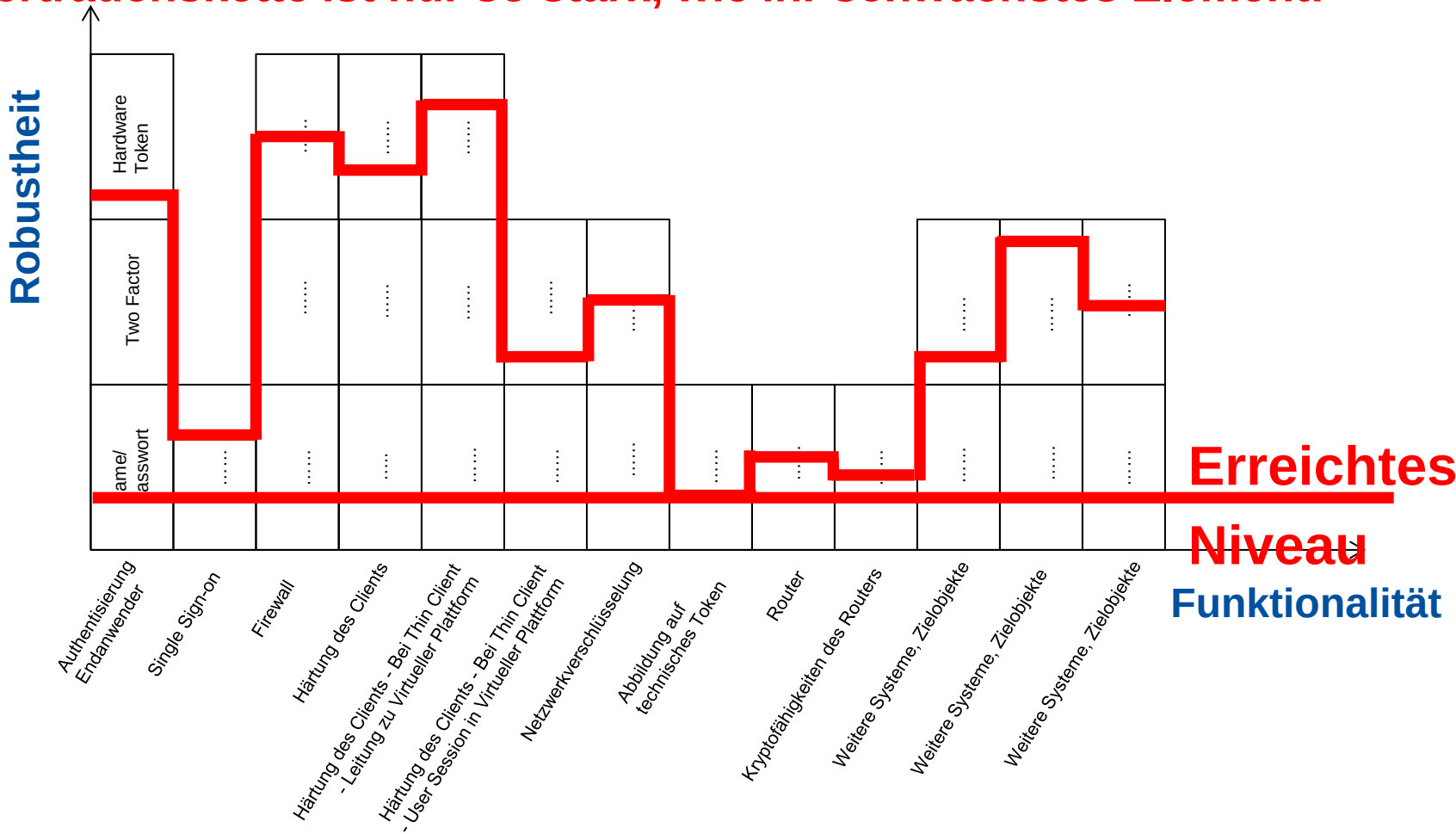


Funktion ohne Schutz ist wertlos!



Vertrauenskette

Eine Vertrauenskette ist nur so stark, wie ihr schwächstes Element!



Durchgehende Sicherheit

Der Einsatz einzelner Sicherheitslösungen bietet keine gesamtheitliche Sicherheit!

Es fehlen:

- Sichere Integration
- Sichere Konfiguration
- Sicherer Betrieb
- …

Dazu benötigt man

- Durgehende Vertrauensketten in der Planung, der Herstellung, Inbetriebnahme …
- transparente Lieferketten
- …

Wo fehlt es an Know-how?

- Viele IT-Sicherheitsprodukte greifen auf „irgendetwas aus dem Internet“ zurück > Schwachstelle Drittprodukte
- Hersteller von „Non-IT-Security“-Produkten haben sich in den IT-Security-Markt bewegt - „*das ja auch nur IT ist – und so schwer kann das nicht sein*“ – bis zur Vernetzung
- Entscheidungsverfahren um „make or buy“ stellt die Robustheit der Lösungen kein wesentliches Ziel dar.
- …
- D.h. auch in Produkten auf denen steht „IT-Sicherheit“ ist nicht immer das gleiche Maß an IT-Sicherheit drin.
- Eine Metrik wäre gut, so dass der Konsument ohne eigenes Know-how verlässlich entscheiden kann
- => Vertrauenswürdige Handlungsketten sind sinnhaft

Vertrauenskette

Die beste Verteidigung ist eine lückenlos vertrauenswürdige Handlungskette in mehreren Dimensionen:

	Durchgehende, lückenlose Vertrauenskette
Technik	Zusammenfügen der Sicherheitsprodukte zu einer sicheren, durchgehenden Vertrauenskette - von der Tastatur bis zu den Services und Daten – IT-Sicherheitsarchitektur
Organisation	Brückenschlag zwischen den Org-Einheiten (z.B. Einkauf und Technik) und der Technik und dem Anwender
Rechtssicherheit	Verfolgen der Lieferkette unter Berücksichtigung von überlagernden Rechtsräumen (z.B. AGB, Five Eyes …)
Haftung	Wenn die Haftung für erfolgreiche Angriffe nicht durchgesetzt werden kann, muss der proaktive Schutz erhöht werden – wer weiß das und handelt danach?
Lieferkette	Transparenz der Lieferkette und verbindliche Haftung des Lieferanten / Herstellers für die Lieferkette (auch wg. Rechtssicherheit und Haftung)

Ihre Sicherheit …
… unsere Mission

Agenda:

1. Ausgangssituation
2. Das Problem
3. Das Ziel
4. Ausblick

Warum messen?

- Einfache eingängige Metrik erzeugen, Komplexität in der Kommunikation zu reduzieren.
- Unterstützung des Einkaufprozesses > Metrik unterstützt Kommunikation Technik zu CXO / Entscheidungsvorlagen > CXO denkt in KPI
- Unterschiede können auch von Non-IT-Security Experts erkannt werden
- Zustandsbeschreibung ermöglichen:
  - ***Objektive Basis*** schaffen
  - Interpretation ermöglichen
  - Veränderungen wahrnehmen
- Vergleichbarkeit und Transparenz im Markt durch Messgrößen
- Maßeinheiten ermöglichen Kriterien für Standardisierung
- Messung sollte früh (vor dem Schaden) ansetzen > singuläre Pentests sind „zu wenig“
- Umgang mit Messgrößen, mit Reputationssystem und Referenzsystem hinterlegen:
  - Benchmarking;
  - Branchenspezifisch
- Indikatoren für sichere Funktionalität schaffen:
  - Bewertung von Funktionen und
  - ihrer Sicherheitseigenschaften

Wie messen?

- Bei einzelnen Marktteilnehmern durchgeführte Analysen und bereits erreichte Schutzziele könnten in adäquaten, verlässlichen Vertrauensketten kommunizierbar sein. Aktuell sprechen noch nicht einmal die Projekte der BW verlässlich miteinander

- Die verfügbaren Ressourcen – also das kollektive Know-how kann im Sinne einer Metrik effizient genutzt werden: die Chancen, die gerade durch zentralisierte Organisationen wie BWI, Rheinbach, ITZB und viele andere entstehen, und die aktuellen Konsolidierungsvorhaben in diesen Organisationen wirklich nutzen

- Die Kostensenkung durch Synergie kann z.B. bei der Konsolidierung der Bundes-IT im ITZB erheblich sein. Ergebnisse müssten dann auch so kommuniziert werden, dass sie für andere Teilnehmer ebenfalls nutzbar werden. (Branchenverbände als „*Übersetzer*“ für die Branchen) – Grundlage Metrik
- …

(Minimaler) Standard

- Definition von Themenspezifischen (Mindest)-standards der Robustheit
- Es ist einfacher einen standardisiert gehärteten Client „aus dem Regal“ zu nehmen, als in jedem Projekt wieder einen „adäquat“ gehärteten Client zu entwickeln – vor allem reduziert sich für den Projektleiter die Komplexität
- Es ist noch einfacher, wenn der gehärtete Client einen Index entlang einer Metrik hat z.B. zwischen 1 und 100 oder entlang einer Indizierung VS – evtl. unterteilt in die verschiedenen Sektoren wie Vertraulichkeit, Haftung, „Stabilität“ der Lieferkette etc.
- ...

Research Themen?

- Wie lassen sich die relevanten Messgrößen aus den verschiedenen Tests sinnvoll zusammenfassen?
- Wie können wir den Lieferanten der Daten geeignet bewerten?
- Wie wirkt sich die gemessene Sicherheit auf die Handlungskette aus? Reseller, Integratoren, Berater, …
- Was gibt es schon für Standards, Metriken und Methoden am Markt?
- Vermarktung der Messgrößen – Plakativ – Verständlich - Geeignet zur Situationsbeschreibung?

Ihre Sicherheit …
… unsere Mission

Agenda:

1. Ausgangssituation
2. Das Problem
3. Das Ziel
4. Ausblick

Was könnte MK tun?

- Darstellen der Zusammenhänge für politische Akteuere und Verbände und
- Motivation der Stakeholder zur Aktion
- Zusätzlich zur Threat-Landscape eine Protection Landscape bei den Stakeholdern anregen.
- Themenabend Cyber Security mit konkreten Handlungsempfehlungen
- Weitere?

Besten Dank für Ihre Aufmerksamkeit