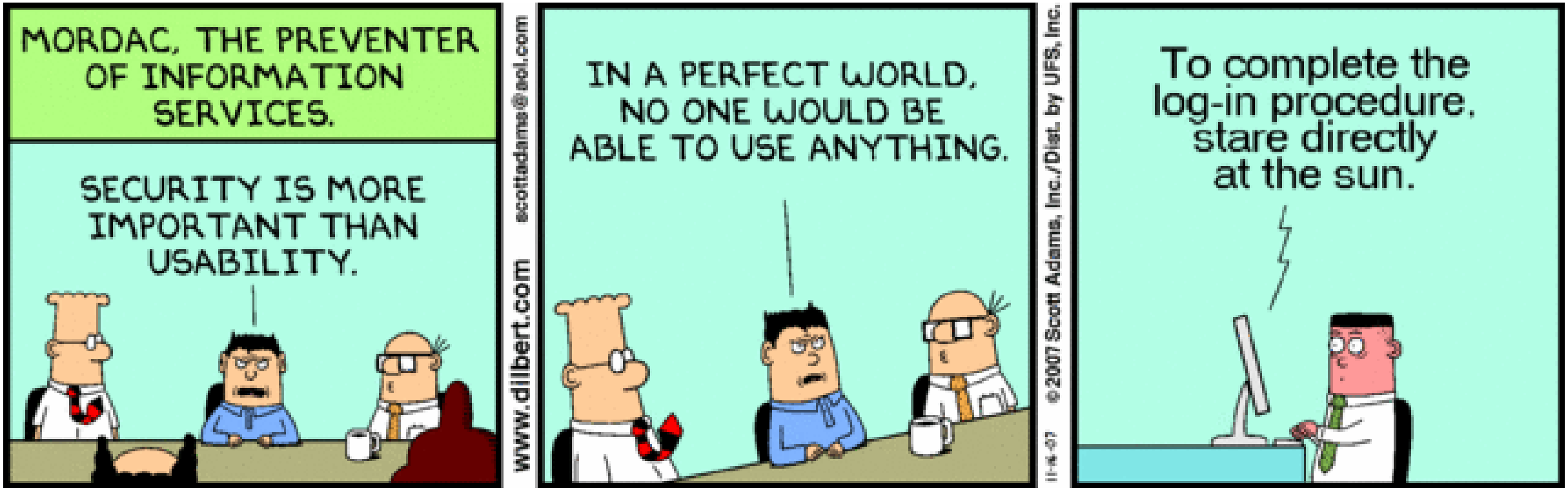
Handlungsbedarf - kein Neuland

Industrie & Security 4.0

Marcel Kisch
IBM Industrial Security Lead DACH

Berlin, 30.06.2014

No-Sense controls



www.dilbert.com

Aus der Prüfung von Security@Industrial

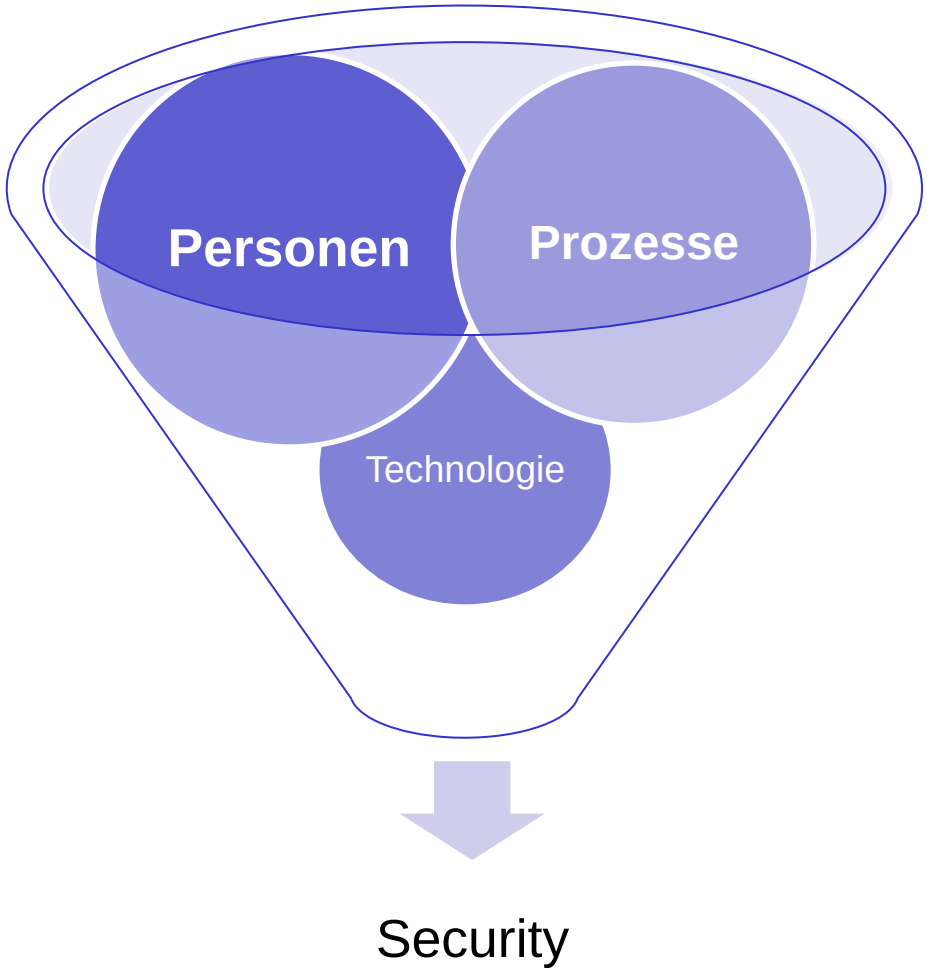
- Unternehmen handeln…
  - bei Bedarf (Sicherheitsvorfall, Risikomanagement)
  - proaktiv wenn Haftung droht oder reaktiv wenn ausreichend Kunden abwandern
  - abhängig ihres organisatorischen Reifegrad
  - nach bestem Wissen und Gewissen

- Standards
  - Vielfältig vorhanden, zum Teil schon sehr lange, etwa ISA-99
  - Kaum ganzheitliche Ansätze, Verwaltungs- und Fertigungs-Standards sind nicht abgestimmt
  - „Einzelempfehlungen“ werden der internen und externen Vernetzung nicht gerecht

➢ Standards: Unverbindlich, nicht harmonisiert, keine Reifegradberücksichtigung für Unternehmen

Elemente wirksamer Security nach Priorität

- Personen
  - Erkennen neues, ist flexibel einsetz- und sensibilisierbar
  - Aber: Gehirn kann sich selbsttätig abschalten
- Prozesse
  - Wirken ordnend und überprüfend,
  - je nach Ausprägung auch nachhaltig steuernd
  - Häufig unternehmensindividuell und abhängig von Reifegrad und Strategie
- Technologie
  - Automatisierbar
  - Keine Tätigkeit ist zu langweilig



➢ Security entsteht im Zusammenspiel aller Elemente

Ursachen von Sicherheitsbrüchen im Industrie-Netz

…sind überschaubar:

- Fehlerhafte Betriebsprozesse
- Designschwächen der Software
- Fehlkonfiguration
- (Veraltete Software)

Wer entdeckt eine Schwachstelle?

- Der Hersteller: Gutes Zeichen
- Externe - und der Hersteller setzt schnell um: Gutes Zeichen

www.heise.de

Industrie 4.0 – Risiken erhöht

- Erzeugung individueller Produkte und Services – und Security!
- Die Wertschöpfung erfolgt
  - Automatisiert und dynamisch,
  - in Form von Massenfertigung – zu hoher Effizienz,
  - flexibel in Echtzeit

- Anwender erwarten
  - standardisierte Komponenten bei standardisierter Kommunikation
  - ➢ Ideale Voraussetzungen für Wettbewerb und technische Security-Maßnahmen

- Durch zunehmende Integration wertschöpfender Systeme = Ausweiterung systemkritischer Infrastruktur = Security-Risiken steigen

Vorschläge für Security 4.0

- Bewusstsein für Security schaffen – notfalls durch Vorgaben (Basel 1-3)
- Security by Design als Chance für Industrie 4.0
- Klare Verantwortlichkeiten (Hersteller, Betreiber, Integrator, …)
- Harmonisierung mit bestehenden Security-Maßnahmen
- Ganzheitliche Betrachtung von Security im Unternehmen
  - Schritt 1: Die Produktion muss das heutige Sicherheitsniveau der Verwaltung erreichen
  - Schritt 2: Die Produktion muss besser abgesichert werden wie die Verwaltung
- Angemessene Balance von Security und Nutzbarkeit
- Definierte Mindestanforderungen an Security (personell, prozessual und funktional)

Klassiker

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”

– Bruce Schneier, "Secrets and Lies", 2000

Vielen Dank!

Marcel Kisch
marcel.kisch@de.ibm.com