the information security provider

Angriffe auf kritische Infrastrukturen

Matthias Hofherr, 12.11.2015

Stuxnet

Hellsing

Duqu

Equation Group

APT 1

APT 17

Regin

Hammertoss

CosmicDuke

MI5: „We are 48h away from anarchy“

APT28

Duqu 2.0

Dragonfly

Winnti

APT 30

Wild Neutron

Sandworm

FinSpy

NetTraveler

Crouching Yedi

Angriffsvektoren

- Spearphishing + Zero Days
- Update-Server von Herstellern
- Schlecht gesicherte ICS-Systeme
- Im Internet exponierte Systeme
- Custom Code >> Byebye AV

Lessons Learned

- Logos sind wichtig ☺
- Angriffe häufen sich
- Immer mehr Angriffpfade
  - Standardkomponenten
  - “Internet der Dinge”
- Freund und Feind lässt sich kaum noch unterscheiden
- Spionage kann auch zu Blackout führen
- Nicht jeder Angriff ist ein APT (auch wenn das viel bequemer ist)

Gesetzliche und regulatorische Vorgaben

- IT-Sicherheitskatalog
  - Spezifisch für Energienetzbetreiber (Gas/Strom)
  - ISMS nach ISO 27001, mit Zertifizierung (aber eigenes Zertifikat)
  - Unabhängig von Größe und Anzahl der Kunden des Unternehmens
  - Ansprechpartner der BNetzA, muss gemeldet werden
  - Seit August 2015 in Kraft

Gesetzliche und regulatorische Vorgaben

- IT-Sicherheitsgesetz
  - Ziel: Kritische Infrastrukturen (genaue Definition ausstehend; Erwartung: ca. 2000 Unternehmen in DE)
  - Anforderungen: Angemessenheit, Stand der Technik, Meldepflicht
  - Regelmässiger Nachweis der Umsetzung
  - Energieanlagen: eigener Sicherheitskatalog in Arbeit
  - Rechtsverordnung ausstehend, die Details regelt
  - Spannend für Mischbetriebe (Netzbetreiber Strom, Gas, Wasser, …)

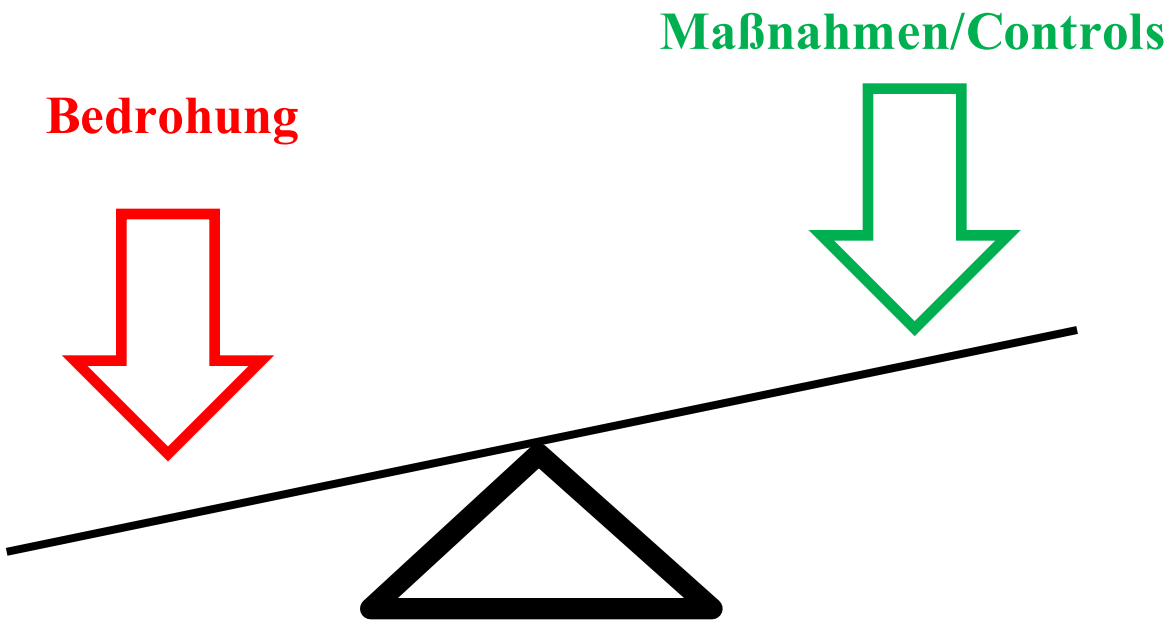
Bewertung

- Was ist mit Dienstleistern/Herstellern?
  - Warum gibt es keine Anforderungen an “sichere Produkte”, z.B. durch Common Criteria-Zertifizierungen?
- Staat != Kritische Infrastruktur?
- Kleine Netzbetreiber >> sehr schwierige Umsetzung
- Erwartungshaltung an ISO 27001 ist optimistisch
  - ISO 27001-Zertifizierung zeigt, dass die richtigen Security-Prozesse implementiert sind, nicht zwingend, dass die Systeme “sicher sind”
  - Der Weg ist das Ziel => “Risikoappetit” wird durch das einzelne Unternehmen festgelegt

Maßnahmen

Offense wins Games – Defense wins Championships

Nur leider momentan nicht in der Informationssicherheit



Maßnahmen

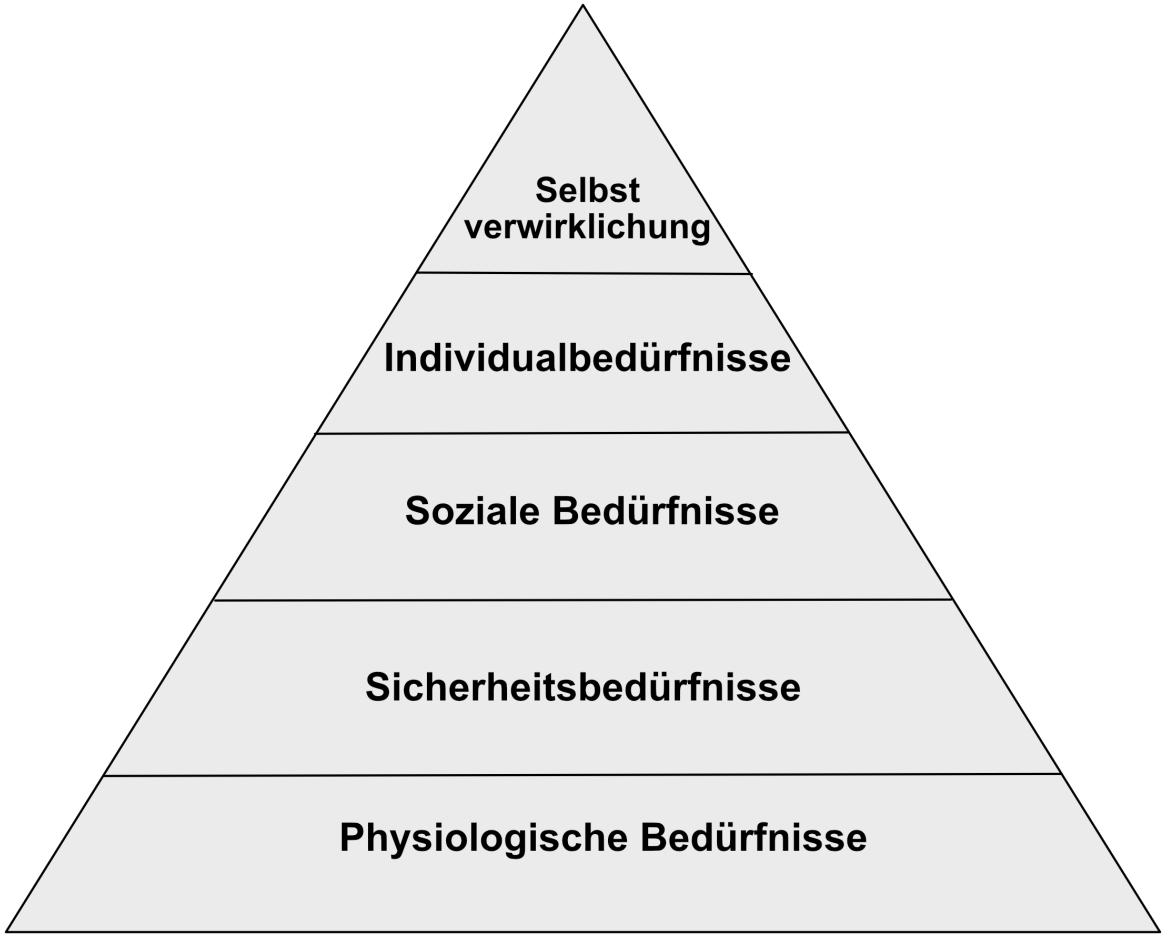
"I am here to tell you that your cyber systems continue to function and serve you not due to the expertise of your security staff but solely due to the sufferance of your opponents"

- Brian Snow 2012

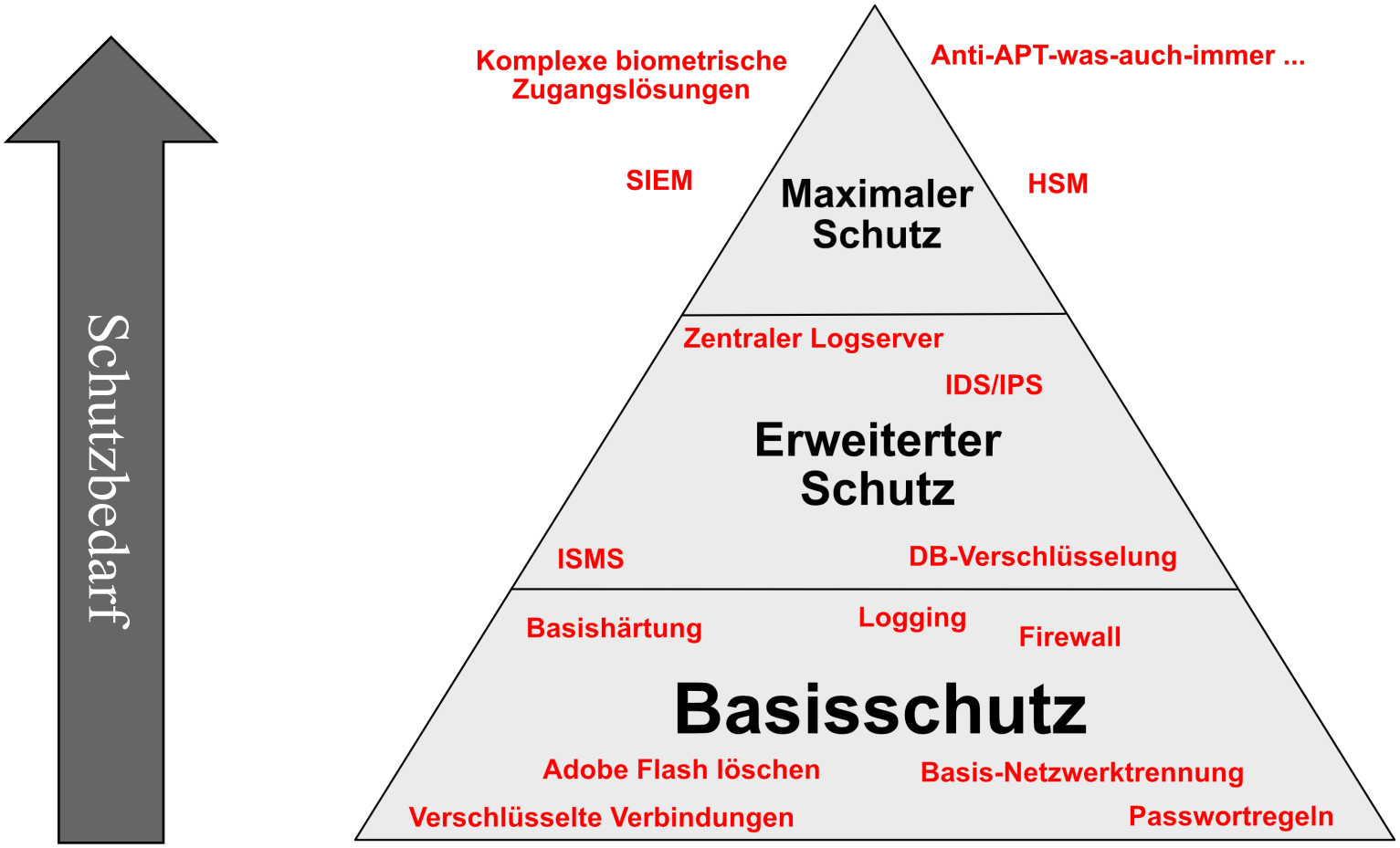
Maßnahmen - Tools

- Es gibt Tools für nahezu alles auf dem Markt
- Weniger ist mehr
- ES GIBT KEINE TURNKEY-SOLUTIONS
- Snakeoil-Alarm!

Maslovsche Bedürfniss-Pyramide



Bedürfnisse der Informationssicherheit



Fazit

- Trotz aller Unkenrufe: ISO 27001 ist eine vernünftige Basis
- Kleinstunternehmen benötigen realistische Implementierungsmodelle
- ISO 27001 darf nicht zur Compliance-Übung verkommen
  => **Compliance sichert keine Systeme**
- Auch die Hersteller müssen in die Pflicht genommen werden