

Methodisches Vorgehen in IT Sicherheitsanalysen

Peter Schoo

`peter.schoo@sit.fraunhofer.de`

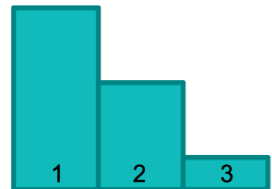
Fraunhofer-Institut für Sichere Informationstechnologie SIT
Garching (bei München)

17. Juni 2010

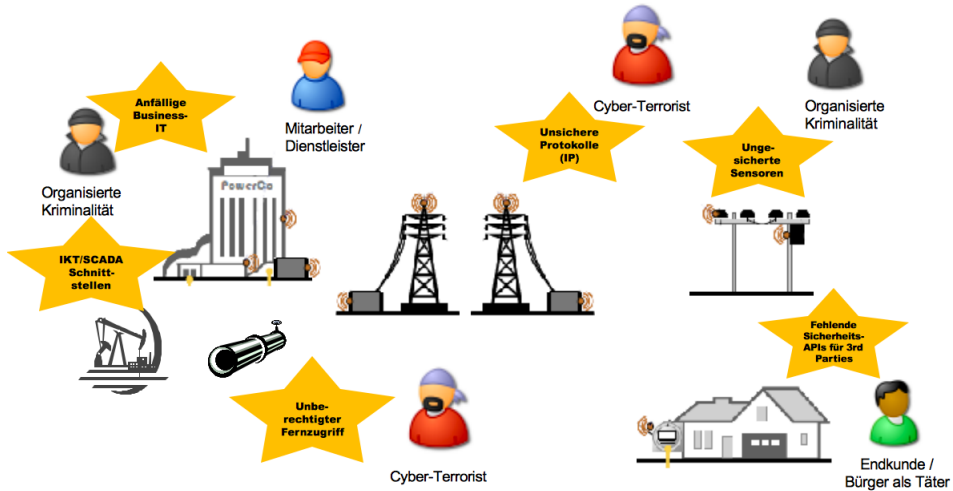
Strategie zur Risiko Minimierung

... in den Grenzen rechtlicher Vorgaben

1. Risiken soweit möglich vermeiden
2. Risiken zu mindern, soweit dies technisch realisierbar
3. Sind verbleibenden Risiken tragbar?



Bedrohungsszenario (unvollständig)



- ▶ Schutzbedarf erfassen
 - ▶ Szenarien-bezogene Bedrohungsanalyse, z.B. Angriffsbäume
 - ▶ Angreifermodelle
 - ▶ Risikomodellierung, z.B. Strömwirkbreite
 - ▶ Verantwortungsbereiche abgrenzen, z.B. Stratifizieren
 - ▶ Referenzarchitekturen konzipieren
 - ▶ Angriffssimulationen

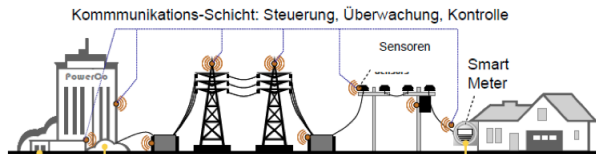
- ▶ Sicherheitsarchitekturen erstellen
 - ▶ Sicherheitstechnologien einsetzen, ggf. Aufwandsprofil gestaffelt
 - ▶ ROSI¹ Betrachtungen
- ▶ Ergebnisse bewerten
 - ▶ Validierung (gem. Auswandsprofilen) → Lösungsgüte
 - ▶ Entwurf Sicherheitsmanagement

¹*Return of Security Investment*

Analysen komplettierende Maßnahmen

IT Sicherheit zur Minimierung der Investitions- und Betriebsrisiken – von Beginn an

- ▶ Methodisch erstellte IT Sicherheitsanalysen helfen sichere, robuste, zuverlässige Systeme zu erstellen
 - ▶ vermeiden persönlicher Präferenzen
 - ▶ mit Sorgfalt und Iterationen zur Vollständigkeit



Analysen komplettierende Maßnahmen

IT Sicherheit zur Minimierung der Investitions- und Betriebsrisiken – von Beginn an

- ▶ Methodisch erstellte IT Sicherheitsanalysen helfen sichere, robuste, zuverlässige Systeme zu erstellen
 - ▶ vermeiden persönlicher Präferenzen
 - ▶ mit Sorgfalt und Iterationen zur Vollständigkeit
 - ▶ **aber:** nicht ausreichend, dem sich täglich ändernden Schutzbedarf zu folgen
→ Bedarf Test- und Demonstrationslabore

