**These: "Sicherheit ergibt sich nur aus Isolation."**

* (Habe ich ja fast so dargestellt.)
* Stimmt das? Andere Aspekte?
* Angriffsweg des Users nicht betroffen.
* ASRL: Address-Space-Layout-Randomisation als Abhilfe?

**Ist diese Klassifizierung sinnvoll? Erfüllt sie ihren Zweck? (welchen?)**

* Nach welchen anderen Kriterien hätte man sonst klassifizieren können?
* Darstellung der Angriffsrichtungen, zur Klärung der Frage, welche man im VNE adressieren kann

**Wahl des Verfahrens? Welche Szenarien gibt es?**

* Telekom -> (Geschichte von Michael) -> einmal virt. dann relativ statisch -> Ansatz 1 geeigneter, da nicht regelmäßig alles ausgetauscht werden muss.
* InP / Webhoster etc. -> Viele neue Request, alte auslaufend -> Ansatz 2. -> Isolation leicht in Vektor integrierbar.
* \* Nach welchen Kriterien kann/sollte man sich für einen Algorithmus entscheiden?  
  \* Nach welchen Kriterien soll der VNE-Algorithmus das Mapping durchführen?

**Mögliche Entwicklungsrichtungen**

* Sicherheitconstraints -> es werden mehr. -> Flexibel bleiben. Neue Exploits entgegenwirken
* Performance
* Wie häufig wird der Alg. eingesetzt.
* Berechnungsart -> KI, Machinelearning (Durchschnittliche Lebenszeit, Sicherheitsanforderungen, freizuhaltende Kapazitäten, "Zukunftsfähigkeit"[Erfahrungsgemäß kommt bei solchen Kunden nach zwei Wochen eine Kapazitätsupgradeanfrage], Wiederkehrende Hochlastsituationen)

**Welchen der Sicherheitsrisiken kann mit Ansatz 1, welchen mit Ansatz 2 begegnet werden?**

* Ansatz1: Isolationsverletzungen
* Ansatz 2: dies auch + x.
* Effektiv? Effizient?