**Inhalt für die Präsentation**

**Einleitung**

* Problem: Anforderungen an die Netzstruktur ändern sich häufig. Beispiel Webhosting. Neuer Kunde möchte vier Maschinen, die zueinander auf bestimmte Weise verlinkt sind. Anbieter kann nicht täglich neue Kabel verlegen oder für jeden Kunden eigene Rechner aufstellen, deren Kapazitäten nicht vollständig ausgelastet werden.
* Vorteile der NV:
  + Abstraktion von der eingesetzten Hardware; Logisches Netzwerk
  + Flexibilität in der Konfiguration des Netzwerks
  + Testumgebungen
  + Automatisierbarkeit; Dynamisches Skalieren
  + Trennung ins InP und SP­
* Herausforderung ist die Zuordnung von virtuellen zu physischen Knoten und Links -> VNE
* VNE wurde bislang nur hinsichtlich Performance optimiert
* Sicherheitsaspekte dabei meist außer Acht gelassen.
* Gliederung dieses Vortrags:
  + Klassifizierung von Sicherheitsrisiken; einigen derer kann bereits im VNE-Alg. begegnet werden
  + Zwei SVNE-Algorithmen vorstellen, die Sicherheitsaspekte integrieren
  + Dazu beginnen wir mit einer kurzen allg. Darstellung des VNE-Prozesses

**Klassifizierung von Sicherheitsrisiken**

* Virtuelle Netzinfrastrukturen sind über die herkömmlichen Gefahren hinaus bedroht.
* Zur Klassifizierung orientierten wir uns an der drei Schichten Architektur des NV
* <BILD: Drei Schichtenarchitektur> + Erklärung:
  + Trennung von ISP in InP und SP
  + Substratnetz zweier InPs hostet zwei virtuelle Netze eines SPs
  + Neun Angriffsrichtungen. Einige eröffnen keine neuen Gefahren
* Unsere Klassifizierung:
* <BILD: Klassifizierung>