**Sicherheitsrisiken virtualisierter Systeme**

**Kapitelgliederung**

1. Kapiteleinleitung
   1. Über die Gewählte Klassifizierung
2. Herkömmliche Gefahren (in Netzinfrastrukturen)
3. (Spezielle Gefahren bei | Neue Verwundbarkeiten in) virtualisierten Umgebungen
   1. User Angriffe auf VN und SN
   2. VN gegen SN
   3. SN gegen VN
4. VNE-Relevante Gefahren

**Kapiteleinleitung**

Wie im vorherigen Kapitel gesehen bietet Netzwerkvirtualisierung einige Vorteile gegenüber bisherigen Netzarchitekturen. Durch die Einführung einer weiteren Schicht zwischen Hard- und Software[Siehe Abbildung] und dem gemeinsamen Hosten verschiedener virtueller Netzwerke auf gemeinsamen Substratnetz tun sich aber auch verschiedene neue Verwundbarkeiten auf.

Diese Verwundbarkeiten lassen sich in unterschiedlicher Weise klassifizieren.

<Abbildung: Drei Layer: Substrat, Virt. und „User“layer>

**Ausformulierte Kapitelgliederung**

**Klassifizierungen**

* Mögliche Klassifizierungen? Für welche entscheide ich mich und warum?

**“Alltagssicherheitsprobleme” [PAPER: When virtual is harder then real…]**

* Virtuelle Maschinen entstehen schnell.
  + Probleme bei Patchmanagement
* VMs zeitweise/Häufig deaktiviert/offline
  + Erhalten keine Patches am Patchday.
  + Würmer infizieren meist relativ schnell alle Verwundbaren Systeme. Geht die VM danach offline wird Malware darin nicht entfernt und die Wurminfektionwelle startet beim erneuten Onlinegehen der VM.
* Rücksetzen/rollback einer VM kann zwischenzeitlich gepatchte Schwachstellen wieder offenbaren
  + Mehr dazu auf [When virtuel is harder then real, S. 4]

**Risiken virtualisierter Systeme**

* Klassifizierung: User Angriffe auf VN und SN, VN gegen SN, SN gegen VN
* Folgt in Teilen [PAPER: Virt. Network emb. Trough sec. Risk. Awareness and opt.]
  + Phys. Host gegen VM
    - Phys. Hosts bieten VMs Ressourcen an. Alle Dienste und Anwendungen der VM werden letztlich auf dem phys. Host ausgeführt. Monitoring, Spoofing, Sniffing, Manipulation des legitimen Datenverkehrs oder Einschleusen schadhafter Nachrichten.
    - VMs können sich gegen ihren phys. Host kaum verteidigen, da alle Berechnungen auf ihm ausgeführt werden.
  + VM gegen ihren phys. Host
    - Schadhafte VM kann Verwundbarkeiten des phys. Host über zugeteilte Ressourcen angreifen (Speicher, Netzwerkkarte, CPU-Last,…).
    - Aus ihrer Isolation ausbrechen
    - Nach Eindringen in oder Übernahme des Hosts kann eine schadhafte VM, dann andere Netzwerkressourcen oder -infrastrukturkomponenten angreifen, und so beispielsweise Services anderer VMs oder VNs behindern.
    - DoS gegen phys. Host kann ggfs. mehrere andere gemeinsam gehostete Virtuelle Netzwerke lahm legen.
  + VM gegen andere VMs auf demselben phys. Host
    - In virtualisierten Umgebungen sind einzelne virt. Netzwerke voneinander logisch isoliert. Virt. Maschinen verschiedener virt. Netzwerke können sich aber ggfs. Ressourcen desselben physischen Knotens teilen.
    - Durch Eindringen oder Übernehmen gewisser Ressourcen des gemeinsamen phys. Hosts kann eine schadhafte VM ggfs. Verwundbarkeiten anderer VMs ausnutzen oder side-channel Angriffe starten, um Informationen zu gewinnen oder Daten zu manipulieren. (vs. Vertraulicheit, Integrität)
* Virt. Netzwerkkarten. Jede VM kann potentiell den gesamten Verkehr aller VMs auf dem phys. Netzwerkkarte sehen.
  + Nicht tragbar in großen Unternehmen / Datacentern.
  + Hosten von Services verschiedener Kunden auf selben phys. Maschine
* VM Interkonnektivität

Logging: Daten der VM bleiben ggfs. auch nach Migration auf dem Host.