**Sicherheitsrisiken virtualisierter Systeme**

**Kapitelgliederung**

1. Kapiteleinleitung
   1. Über die Gewählte Klassifizierung
2. Herkömmliche Gefahren (in Netzinfrastrukturen) [ggfs. nicht, bzw. nur kurz]
3. (Spezielle Gefahren bei | Neue Verwundbarkeiten in) virtualisierten Umgebungen
   1. Organisatorisch(er Art)
   2. Rechtlich(er Art)
   3. Technisch(er Art) [<- Hierauf konzentriert]
      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 Hardware und Anwendungssoftware[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: „Substratnetz hostet zwei virt. Netzte“ Layer: Substratnetz, VN1, VN2 (vgl. fischer2011position)> ODER <Abbildung: „Schichtenarchitektur der Netzwerkvirtualisierung“ (vgl. wang2016towards, Fig.1)> ODER <(Vgl. A survey of network virtualization, S. 7)>

<Abbildung: Zusätzliche Layer durch Virtualisierung: Phys. Ress., Virt. Layer, Virt. Ress. VMs (vgl. fischer2011position)> -> Angriffe darin einordnen

<Liste an Papern> haben bereits einige Sicherheitsrisiken analysiert, welche im Folgenden klassifiziert, erläutert und stellenweise ergänzt werden.

**Ausformulierte Kapitelgliederung**

<Graphik zu meiner Klassifizierung + Erläuterung derer. Ggfs. ähnlich dahbur2011survey, S.4>

**Klassifizierungen**

* Mögliche Klassifizierungen? Für welche entscheide ich mich und warum?
  + Mehrere Klassifizierungen parallel?
  + CIA immer dazu gesagt?
* Woraus resultiert die Verwundbarkeit?
  + Virtualisierung, Serviceorientierung
* CIA (goal-based)
* Nach Layer (Phys., Logische, UI)

**“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 (Snapshot-Problem)
  + Mehr dazu auf [When virtual is harder then real, S. 4]

**Technische Verwundbarkeiten virtualisierter Systeme**

* Unterkapiteleinleitung
* Klassifizierung: Organisatorisch, rechtlich, technisch>(User Angriffe auf VN und SN, VN gegen SN, SN gegen VN)
  + (VM gegen VM auf anderen phys. Host dürfte vergleichbar sein mit herkömmlichen Angriffen via Netzwerk.)
* Folgt in Teilen [PAPER: gong2016virtual]
  + 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 („break of isolation“[PAPER -> gong2016virtual?])
    - 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)
    - Ggfs. Monitoring anderer VMs via zugrundeliegendem Substratnetzwerk („break of isolation“)
    - Sniffing via Wirrshark[orebaugh2006wireshark] und Spoofing (z.B. auf ARP-Ebene[whalen2001introduction])
    - Zugangskontrolle?
      * Ungenügendes Zugangskontrollsystem kann root der VM A dazu berechtigen via gemeinsame Ressourcen auf VM B einzuwirken.
* 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
* Gefahr einer Infektion der VM groß, da viele andere VMs potentiell offene Verwundbarkeiten aufweisen (Patchmanagement schwer). Infektion breitet sich via gemeinsame Ressourcen ggfs. schneller aus.
* VM Interkonnektivität

**Weitere Verwundbarkeiten virtualisierter Umgebungen**

* [PAPER: wu2010network, garfinkel2005virtual, dahbur2011survey, gong2016virtual…]
* JEWEILS NOCH WEITER AUSFÜHREN. BEISPIELE.
* „Break of isolation“. VM kann andere VMs monitoren oder in die phys. Hostmaschine eindringen
* Aus der Möglichkeit die gesamte virtuelle Netzwerkumgebung aus der Ferne umkonfigurieren zu können, ergeben sich weitere Verwundbarkeiten durch Cross-site scripting, SQL injection etc. -> Angriffe auf das Management-Tool
* DoS. Gemeinsam geteilte Ressourcen wie CPU, Haupt- und Hintergrundspeicher oder Substratnetzwerk.
* Rootkits. Gewähren root/Admin Zugang zum physischen Host.
  + Wenn Rootkit den Hypervisor kompromittiert, kann Kontrolle über alle gehosteten VMs erlangt werden. (Host gegen VN/VM)
  + VM agiert ggfs. als Rootkit. (VM gegen Host)
  + Vorbereitung für weitere Angriffe (DoS, Sniffing,…)
  + Beispiel BluePill [rutkowska2008bluepilling, (dahbur2011survey)]
* Snapshot-Problem. Momentanaufnahme der virt. Maschine für Backup- oder Migrationszwecke.
  + Einfachheit dessen ist großer Vorteil von VMs.
  + Nachteil: Nach dem Wiedereinspielen werden ggfs. zwischenzeitlich deaktivierte Accounts oder veraltete Sicherheitsrichtlinien wieder produktiv gesetzt.
  + VGL. „Alltagsprobleme“
* Sniffing
* Spoofing [whalen2001introduction]
* Möglichkeit des Datenleck beim Upload/Download
  + Da virt. Netzwerk oftmals via Cloudcomputing abgewickelt wird.

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

**Organisatorische Risiken**

* Siehe auch „Alltagsgefahren“
* Reputationsverlust des Unternehmens, wegen Aktivitäten der anderen Unternehmen der Personen, mit denen es einen phys. Host teilt.
  + Sicherheitsanforderung „Kein Kohosting (mit XY)“ -> nur 1 VM pro phys. Host -> Kein z.B. Preisvorteil…
* Substratnetzprovider ist auch ein Unternehmen/Dienstleister, der sich organisatorisch verändert oder z.B. Insolvenz anmelden kann.
* Ggfs. muss ein Unternehmen, um bei unerwarteten Lastspitzen (oder DDoS-Angriffen) Verfügbarkeit gewährleisten zu können, über das Angebot an den Sicherheitsrichtlinien des Unternehmens entsprechenden phys. Hosts hinaus skaliert werden. Die Möglichkeit der Skalierbarkeit verleitet womöglich in Situationen, in denen anderweitig ein Ausfall hinzunehmen wäre, dazu Sicherheitsrichtlinien zu unterwandern.

**Rechtliche Risiken**

* Da Substratnetze nicht zwingend räumlich eng beschränkt sein müssen, könnte es passieren, dass gewisse Teile des Virtuellen Netzes in ein Land gemappt werden, welches mit den Auflagen des Unternehmens zu Datenschutz, Privatsphäre oder IT-Securitystandards nicht vereinbar ist.