**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. Technisch(er Art) [<- Hierauf konzentriert]
      1. ~~User Angriffe auf VN und SN <- ??? (= Herkömmliche Gefahren?)~~
      2. ~~VN gegen SN~~
      3. ~~SN gegen VN~~
      4. ~~VM gegen andere VMs auf demselben phys. Host~~
      5. Von NI
         1. Gegen NI
         2. Gegen VN/VM
         3. Gegen User
      6. Von VN/VM
         1. Gegen NI
         2. Gegen VN/VM
         3. Gegen User
      7. Von User
         1. Gegen NI
         2. Gegen VN/VM
         3. Gegen User
   2. Organisatorisch(er Art)
   3. Rechtlich(er Art)
4. VNE-Relevante Gefahren

**Kapiteleinleitung**

Wie im vorherigen Kapitel [KAPITELNUMMER] 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. Eine Klassifizierung solcher wird in diesem Kapitel unternommen.

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>

Definition: ‚Risiko‘ vs. ‚Verwundbarkeit‘ vs. ‚Gefahr‘ vs. ‚Bedrohung‘

**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)
* Meine Klassifizierung: technisch>i, ii, iii | orga | rechtlich.
  + Unter Einbezug von CIA am jeweiligen Ort.
  + Hauptaugenmerk auf ‚aus Virtualisierung resultierende Gefahren‘
* (VM gegen VM auf anderen phys. Host dürfte vergleichbar sein mit herkömmlichen Angriffen via Netzwerk.)

Sicherheitsrisiken in virtualisierten Netzinfrastrukturen lassen sich auf verschiedene Weisen wie z.B. nach ISO/OSI-Schicht, nach Verletzung der klassischen C.I.A.-Aspekte, [nach Schicht in der NV-Architektur,] oder aus Sicht des SPs bzw. InPs klassifizieren. Da dieses Kapitel sich aber auf durch Netzvirtualisierung gegenüber herkömmlichen Netzinfrastrukturen neu hinzukommende Risiken konzentriert, liegt der folgenden Klassifizierung zur Verdeutlichung der Angriffswege die in Abbildung [ABBILDUNG Klassifizierung] dargestellte Struktur zugrunde.

KLASSIFIZIERUNGSBESCHREIBUNG AKTUALISIEREN!

Sicherheitsrisiken werden zunächst nach solchen technischer, organisatorischer bzw. unternehmerischer und rechtlicher Art gegliedert. Im Zentrum der Betrachtung stehen dabei die technischen Risiken, welche wiederum nach Angriffsrichtungen ‚Physischer Host gegen VN/VM‘, ‚VM gegen ihren physischen Host‘ und ‚VM gegen andere VMs auf demselben physischen Host‘ unterteilt werden sollen.\footnote{Die Betrachtung von ‚VM gegen VMs auf anderen physischen Hosts‘ dürfte vergleichbar mit herkömmlichen Angriffen in Netzinfrastrukturen sein und wird daher an dieser Stelle nicht ausgeführt.}

Definition: Was sind ‚herkömmliche Gefahren‘? Welche Kategorien werden nicht betrachtet?

Folgt in Teilen [gong2016virtual, natarajansecurity, wu2010network, garfinkel2005virtual, dahbur2011survey]

**Was Widerspricht Anforderungen aus Kapitel ANFORDERUGNEN?**

**VON NI**

**Von NI / Physischer Host gegen VN/VM und Endsysteme**

Physische Hosts bieten ihren VMs Ressourcen an. Alle Dienste und Anwendungen der VMs werden letztlich auf dem physischen Host ausgeführt und auch alle Daten auf ihm gespeichert. Dies eröffnet für den physischen Host prinzipiell die Möglichkeit eines Monitorings der VM-Aktivitäten, was ab einer gewissen Intensität sicherlich über Verwaltungsbelange hinausgehen und Privatsphärenanforderungen widersprechen dürfte. Auf demselben Weg lassen sich auch vertraulichkeitsverletzende Sniffing- oder Spoofing-Attacken gegen VM bzw. VN starten.

Da alle ihre Rechenoperationen letztlich auf dem physischen Host ausgeführt werden, ist es für eine VM nur schwer möglich sich gegen solche Angriffe zu wehren. [VERSCHLÜSSELUNG ALS AUSWEG?]

Auch Manipulation des legitimen Datenverkehrs, (gezieltes) Verwerfen von empfangenen Paketen bzw. das Einschleusen schadhafter Nachrichten bieten eine weitere Möglichkeit der Kompromittierung, gegen die VNs und Endsysteme wohl schutzlos ausgeliefert ist.

[AUSFÜHRLICHER?]

Durch derartige Aktionen oder auch unzureichende Sicherungsmaßnahmen gegen Datenabfluss kann der physische Host in den SLAs vereinbarte Bestimmungen verletzen, was gerade bei Drittanbietern als Hostingpartner eine Rolle spielt.

%%%%% Angriffe von Komponenten der NI untereinander werden hier nicht beachtet.[Bereits weiter oben sagen.]

**VON VN/VM**

**Von VM / VM gegen ihren physischen Host / NI**

Das Bereitstellen von Ressourcen für VMs ist aber auch für den physischen Host nicht ohne Risiko. Schadhafte oder bösartige VMs können Verwundbarkeiten ihres physischen Host über zugeteilte Ressourcen angreifen. Ohne hinreichende Restriktionen könnte eine VM dann über ihr zugeteiltes Kontingent hinaus bspw. wichtige Speicherbereiche manipulieren oder durch übermäßige Reservierung von CPU-Zeiten eine Denail of Service Attacke gegen den physischen Host bzw. das Substratnetz fahren. Da Host und virtuelle Netztopologie aus der Ferne konfigurierbar sind, stellt das Einschleusen von konstruierten Nachrichten des verwendeten Netzwerkmanagementprotokolls auf oder durch die Netzwerkkarte des physischen Hosts einen weiteren gefährlichen Angriffsvektor dar.

Nach Eindringen in oder Übernahme des Hosts, einem „break of isolation“ im ersten Sinne \cite{wu2010network}, könnte eine schadhafte VM dann ihr Kontingent an Ressourcen beeinflussen, netztopologische Informationen sammeln, andere Netzwerkressourcen oder -infrastrukturkomponenten angreifen und so beispielsweise Dienste anderer VMs oder VNs behindern.

VM kann als Rootkit agieren.[wu2010network. Dazu mehr unter ‚User gegen NI‘]

VM gegen Host -> Belauschen von Netzwerkverkehr anderer. Service reproduzieren (z.B. live Video Streaming) (=Übergang zu VN gegen VN?)

**VM/VN gegen VM/VN**

Neben den herkömmlichen Angriffsszenarien zwischen Maschinen im selben Netzwerk, ergeben sich v. a. aus der gemeinsamen Nutzung von Ressourcen neue Angriffsvektoren. Ein Angreifer kann sich nun gezielt Ressourcen auf denjenigen physischen Maschinen mieten, von denen auch sein Angriffsziel gehostet wird, um so erleichterten Zugang zu deren Verwundbarkeiten zu erlangen. Durch Eindringen oder Übernehmen gewisser Ressourcen des gemeinsamen physischen Hosts kann eine schadhafte VM dann ggfs. Verwundbarkeiten ausnutzen oder durch Cross-VN-side-channel-Attacken vertrauliche Informationen gewinnen und Daten manipulieren. Ein Beispiel einer Integritätsverletzung mittels einer solchen Attacke findet sich in \cite{ristenpart2009hey}.

Da i.d.R. [ANGABE?] werden nur virtuelle Netzwerkkarten zugeteilt, kann jede VM potentiell den gesamten Datenverkehr aller VMs bzw. VNs auf derselben physischen Netzwerkkarte lesen. Ein Monitoring anderer VMs auch aus anderen VNs, ein „break of Isolation“ im zweiten Sinne bedroht deren Vertraulichkeit.

Sollte es einer VM gelingen kritische Teile ihres physischen Hosts zu übernehmen, so stehen ihr zusätzlich die im Abschnitt [VON PHYSISCHER HOST GEGEN VN/VM UND ENDSYSTEME] aufgeführten Angriffsvektoren offen.

**VM gegen User**

Einschleusen von Nachrichten zur Störung oder Abbruch von z.B. TCP-Verkehr/P2P-Verbindungen

Übliche Methoden der Einflussnahme auf den Nutzerverkehr -> Herkömmlich

KATEGORIEN ‚von/gegen User‘ KLARER UNTERSCHEIDEN VON ‚von/gegen VN‘

**VON USER**

**Von User gegen NI**

**Von User gegen VN**

**Von User gegen User**

**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.
    - SLAs verletzen (v.a. wenn bei Drittanbietern gehostet)
  + VM gegen ihren phys. Host
    - Schadhafte VM kann Verwundbarkeiten des phys. Host über zugeteilte Ressourcen angreifen (Speicher, Netzwerkkarte, CPU-Last,…).
    - DoS gegen phys. Host kann ggfs. mehrere andere gemeinsam gehostete Virtuelle Netzwerke lahm legen. (DoS gegen phys. Host)
    - Aus ihrer Isolation ausbrechen („break of isolation“ im ersten Sinn [PAPER -> wu2010network, 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.
    - Bösartige VM belegt übermäßig Ressourcen -> beeinträchtigung Cohostet VMs.
    - VM gegen Host -> Belauschen von Netzwerkverkehr anderer. Service reproduzieren (z.B. live Video Streaming)
  + VM gegen andere VMs auf demselben phys. Host
    - Durch die gemeinsame Nutzung von Ressourcen ergeben sich neue Angriffsmöglichkeiten. Ein Angreifer kann sich ~~eine gewisse Menge an~~ Ressourcen auf denjenigen physischen Maschinen mieten, von denen auch sein Angriffsziel gehostet wird, um so Zugang zu deren Verwundbarkeiten zu erlangen, oder um durch Cross-VN-side-channel-Attacken vertrauliche Informationen zu gewinnen oder Daten zu manipulieren. Ein Beispiel einer Integritätsverletzung mittels eines solchen Angriffs findet sich in \cite{ristenpart2009hey}.
    - Durch Eindringen oder Übernehmen gewisser Ressourcen des gemeinsamen phys. Hosts kann eine schadhafte VM ggfs. Verwundbarkeiten anderer VMs ausnutzen oder side channel Angriffe[ANGABE?] starten, um Informationen zu gewinnen oder Daten zu manipulieren. (vs. Vertraulicheit, Integrität)
      * DoS. Gemeinsam geteilte Ressourcen wie CPU, Haupt- und Hintergrundspeicher oder Substratnetzwerk. (vs. Verfügbarkeit)   
        (DoS gegen andere VMs via DoS gegen Host oder via gezielte Exploits gegen einzelne VMs bzw. gegen Netzwerkkarte)
    - Virt. Netzwerkkarten. Jede VM kann potentiell den gesamten Verkehr aller VMs auf dem phys. Netzwerkkarte sehen. (vs. Vertraulichkeit)
      * Nicht tragbar in großen Unternehmen / Datacentern.
      * Hosten von Services verschiedener Kunden auf selben phys. Maschine
    - Ggfs. Monitoring anderer VMs via zugrundeliegendem Substratnetzwerk („break of isolation“ im zweiten Sinn) [wu2010network]
      * „Break of isolation“. VM kann andere VMs monitoren oder in die phys. Hostmaschine eindringen
    - Sniffing via Wireshark[orebaugh2006wireshark] und Spoofing (z.B. auf ARP-Ebene[whalen2001introduction])
    - Gefahr einer Malewareinfektion der VM groß, da viele andere VMs potentiell offene Verwundbarkeiten aufweisen (Patchmanagement schwer[erst später sagen]). Infektion breitet sich via gemeinsame Ressourcen ggfs. schneller aus.
    - In virtualisierten Umgebungen sind einzelne virt. Netzwerke voneinander logisch isoliert. Virt. Maschinen verschiedener virt. Netzwerke können sich aber ggfs. Ressourcen desselben physischen Knotens teilen.
      * Auf diese Weise können sich Infektionen auch über Grenzen des virt. Netzes / auch auf andere virt. Netze ausbreiten.
    - Zugangskontrolle?
      * Ungenügendes Zugangskontrollsystem kann root der VM A dazu berechtigen via gemeinsame Ressourcen auf VM B einzuwirken.
    - Wenn VM den Host kontrolliert, dann auch andere VMs auf selben Host (siehe Teil ‚phys. Host gegen VM‘)
  + VM Interkonnektivität

**TABELLE MIT RISIKEN?! (vgl. wang2016towards) -> Referenzierung im Kapitel „VNE-relevant“**

**Weitere Verwundbarkeiten virtualisierter Umgebungen**

* [PAPER: wu2010network, garfinkel2005virtual, dahbur2011survey, gong2016virtual…]
* JEWEILS NOCH WEITER AUSFÜHREN. BEISPIELE.
* 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 werden lohnend
* 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)]
* **GEFAHREN IM UMGANG MIT VMs**
* 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.
  + 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]
* 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 oder Personen, mit denen es einen phys. Host teilt.
  + Sicherheitsanforderung „Kein Kohosting (mit XY)“ -> nur 1 VM/Kunde pro phys. Host -> Weniger z.B. Kostenvorteil…
* 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 (dynamisch / lastbedingt) in ein Land gemappt werden, welches mit den Auflagen des Unternehmens zu Datenschutz, Privatsphäre oder IT-Securitystandards nicht vereinbar ist.
* Aus technischen Gefahren resultierende Risiken (Sniffing vs. Datenschutz, Leaks, …)

User = Endsystem / Service, der in VNs implementiert wird oder Nutzer.

NI = Netzwerkinfrastruktur / Substratnetz

* Gegen VN/VM
  + Von User
    - Herkömmliche (User gegen Netzwerk, z.B. manipulierte Nachrichten zur Störung des Netzwerkverkehrs, Erzeugung von Überlast, …)
    - + Während der live Migration eines VNs ist eine Man-in-the-Middle-Attacke möglich, mit der Informationen über und Inhalte des migrierenen VNs erlangt werden können.[Vgl. natarajansecurity, S. 18]
    - Sogar die Manipulation von Speicherbereiche von VMs ist während der Migration möglich und lässt sich automatisieren.[oberheide2008empirical]
  + Von anderer VM/VM
  + Von Host
    - Manipulation von Verkehr.
    - SLAs verletzen (v.a. wenn bei Drittanbietern gehostet)
* Gegen Host
  + Von User
    - Überfluten -> DoS. (Herkömmloch)
    - Netzwerkkomponenten wie Switches und Router sind dynamisch (um)programmierbar -> nötig für VNE. Codeexpliots wie Bufferoverflows etc.) -> DoS.
  + Von VN/VM
    - Bösartige VM belegt übermäßig Ressourcen -> beeinträchtigung Cohostet VMs.
    - VM gegen Host -> Belauschen von Netzwerkverkehr anderer. Service reproduzieren (z.B. live Video Streaming)
  + Von anderen Host -> Herkömmlich
* Gegen User
  + Von User -> Herkömmlich
  + Von VN
    - Einschleusen von Nachrichten zur Störung oder Abbruch von z.B. TCP-Verkehr/P2P-Verbindungen
    - Übliche Methoden der Einflussnahme auf den Nutzerverkehr -> Herkömmlich
  + Von Substratnetz

Host gegen VM/VN

VN/VM gegen Host -> BluePilling(?)

VM gegen VM

User gegen Substratnetz -> herkömmlich

User gegen VN/VM -> herkömmlich

User gegen VN via Substratnetz - > BluePilling(?), SQL-Injektion der Managementsoftware

Substratnetz gegen User

VN gegen User