**Sicherheitsanforderungen**

**Kapitelgliederung**

1. Kapiteleinleitung
2. Sicherheitsanforderungen
   1. Von SP/User an InP
   2. Von InP an SP/User
3. Überleitung

**Kapiteleinleitung**

Netzwerkvirtualisierung ist eine Methode unabhängige und voneinander isolierte logische Netzwerke auf einem gemeinsamen physischen Netzwerk zu betreiben.

Anforderungen gehen mit Risiken einher.

**(Sicherheits-)anforderungen an virtualisierte Umgebungen**

* Anonymität und Privatsphäre von Nutzern (vertrauenswürdige Paketweiterleitung, wenn das virt. Netzwerk bei einem Drittanbieter gehostet ist)
* VM Interkonnektivität
* Möglichkeit zur Zusammenarbeit mit nicht-virtualisierten Netzen und Anwendungen
  + Bsp. Günstige Webhosting-Lösungen auf vServern sollen auch von nicht-virt. Maschinen aus erreichbar sein.
* Angriffe von Endnutzern sollten nicht in der Lage sein das Substratnetz zu beeinträchtigen, während Attackenverkehr hingegen identifiziert und gefiltert werden können soll.
* Substratnetz sollte nicht VN-Verkehr monitoren, sniffen, manipulieren, stören/unterbrechen (können).
* Umgekehrt sollte auch das VN keine Informationen über das Substratnetz sammeln (können).
* Substratnetz sollte effektive Kontrollmechanismen gegen unerlaubte Erlangung von Infos aus/über das VN bereitstellen.
* …

**Mögliche Richtlinien**

* [In dieser Arbeit werden folgende Begriffe in diesem Sinne verstanden.]
* Vgl. auch [cabuk2007towards]
* Isolation ist Hauptaufgabe / Kernpunkt [-> Ausbauen]
  + Keine gegenseitige Beeinflussung der VMs oder VNs
  + Keine Beeinflussung zwischen VMs verschiedener Mieter / VNs.
  + Von zwei VMs gemeinsam genutzte Ressourcen sind logisch voneinander getrennt. Kein ungewollter direkter Informationsfluss.[Fußnote: Ausführliche Betrachtung indirekten Informationsflusses z.B. via verdeckter Kanäle oder side channel Attacken würde den Umfang dieser Arbeit übersteigen.]
  + Problem: Kunde weiß nicht, ob die „Nachbar-VM“ vertrauenswürdig ist.
  + Die gehosteten VNs sollten keine Attacken gegen privilegierte Informationen der Substratinfrastruktur fahren.
* Datenschutz
* Vertraulichkeit, Integrität, Verfügbarkeit (CIA)
  + Vertraulichkeit: Zwei VMs innerhalb desselben VNs sollen in der Lage sein frei miteinander zu kommunizieren, ohne dann dabei ein Dritter durch Belauschung an Kommunikationsinhalte gelangen kann.
  + Integrität: Ein virt. Knoten / VM soll nicht in der Lage sein, (Kommunikations-)Daten Anderer zu manipulieren und die eigene Urheberschaft der Veränderungen einer anderen Instanz zuzuschreiben.
* Informationsflusskontrolle
* Mitglieder- und Zulassungsverwaltung in Virt. Netzen.

**Fragen / Herausforderungen:** [natarajansecurity]

Kann das Substratnetz Paketvermittlung effektiv durchführen, ohne Informationen über das VN zu sammeln oder Privatsphäre zu verletzen?