7.1 Einleitung

Ob in einer physischen oder virtuellen ICT-Umgebung, der Vertraulichkeit, Integrität sowie Verfügbarkeit von Daten und Systemen gebührt oberste Priorität. Die Fachabkürzung für genau diese drei Bereiche nennt sich *CIA* – hiermit ist nicht der ausländische Geheimdienst der USA (Central Intelligence Agency) gemeint. Die Abkürzung CIA steht im Bereich der Informatik für *Confidentiality, Integrity und Availability*.

Für die Sicherstellung dieser drei Punkte, sollten einige Eckpfeiler Ihrer Umgebung erhöhte Aufmerksamkeit geniessen. Die folgenden Teilkapitel werden genau diese paar Bereiche einer virtualisierten Umgebung genauer beleuchten.

7.2 Sicherheit

Die Komplexität verlangt ein höheres Sicherheitsbewusstsein.

Wenn wir von Sicherheit in einer virtualisierten Umgebung sprechen, sprechen wir von neuen Sicherheitslücken. Sicherheitslücken, welche wir aus physischen Umgebungen her so nicht kannten – diese Lücken sind jedoch nicht nur systembedingt, auch lassen Sie sich nicht einzig durch die rassante Entwicklung erklären.

Eines der potenziell grössten (jedoch auch bei physischen Umgebungen vorhandenen) Risiken ist das blinde Vertrauen in ein Stück Software. Wer kann Ihnen garantieren, dass im Hypervisor kein Backdoor[1] eingebaut wurde. Da der Hypervisor die Schnittstelle zwischen VM und Hardware bildet, ist er rein faktisch gesehen im Stande, sämtliche Kommunikation mitzuschneiden.

Nebst dem erwähnten bewussten Einschläusen von *Hintertürchen*, sind Sie (ohne weitere Schutzmassnahmen) allfälligen Softwareschwächen seitens Hypervisor eben so ausgeliefert. Schlecht programmierte Schnittstellen erlauben es zum Beispiel, Systeme zu korrumpieren und für fremde Zwecke zu nutzen (Daten aufzeichnen, Daten manipulieren etc.).

Des Weiteren sollte auch den zuführenden Netzwerkschnittstellen unbedingt Beachtung geschenkt werden. Sind die jeweiligen VM-Netze korrekt voneinander getrennt? Besteht die Gefahr, dass eine virtualisierte Firewall von Seitens des ISP[2]-Zugangs direkt angesprochen werden kann? Bestehen Netzwerkbrücken, wo keine sein sollten?

---

1 Als Backdoor wird ein Stück Software bezeichnet, welches vom Autor bewusst platziert wurde, um Zugriff auf fremede System zu erhalten.

2 Internet Service Provider; Stellt Endkunden den Internetzugang zur Verfügung.