Kurzfassung der Dissertation “Security of Access and Usage of Cloud Infrastructures” von Dennis Felsch

Mit dem Fortschritt der Web-Technologie entstanden Web-Anwendungen, die zunehmend Desktop-Anwendungen ersetzen können. Diese Verlagerung *in die Cloud* wurde unter dem Begriff SaaS (Software-as-a-Service) bekannt. Konsequenterweise wurde auch Rechenleistung als Dienstleistung angeboten, was heute IaaS (Infrastructure-as-a-Service) genannt wird. Dabei waren Diskussionen über Sicherheitsbedenken bei der Nutzung der Cloud immer ein Thema. Die Nutzung von Cloud-Diensten bedeutet in der Regel, dass persönliche und andere sensible Daten unverschlüsselt auf Servern im Internet gespeichert werden, auf die möglicherweise Unternehmen, Geheimdienste oder Cyberkriminelle zugreifen könnten.

Ein häufig unterbreiteter Vorschlag, diesen Risiken entgegenzuwirken, ist die Verwendung einer *Private Cloud*. Diese Dissertation untersucht zu Beginn diesen Vorschlag und legt dar, dass er zwei schwerwiegende Missverständnisse enthält: Zunächst wird gezeigt, dass verbreitete Definitionen des Begriffs Private Cloud den technischen Aufbau nicht berücksichtigen und daher wenig über die technische Sicherheit aussagen. Zweitens zeigen wir, dass Private Clouds nicht immun gegen Angriffe sind: Wir analysieren vier Open-Source-Projekte für den privaten IaaS-Cloud-Einsatz (Eucalyptus, OpenNebula, OpenStack und openQRM). Dabei haben die Webschnittstellen der Private Clouds Anfälligkeiten für etablierte Angriffstechniken wie XSS (Cross-Site-Scripting), CSRF (Cross-Site-Request-Forgery) und Clickjacking gezeigt. Die Sicherheit von drei Cloud Installationen konnte mit neuartigen Exploit-Techniken, die wir für IaaS-Clouds entwickelt haben, kompromittiert werden. Einer der Angriffe ermöglichte es sogar, Root-Zugriff auf VMs (Virtual Machines) zu erhalten, selbst wenn vollständige Perimeter-Sicherheit aktiviert ist. Die Verantwortlichen aller Open-Source-Projekte wurden über die Angriffsvektoren informiert und unsere vorgeschlagenen Gegenmaßnahmen wurden integriert. Als Ergebnis dieser Dissertation wird empfohlen, Webschnittstellen für Private Clouds vom Internet aus nicht zugänglich zu machen und diese technische Anforderung in die Definition einer Private Cloud aufzunehmen.

Wenn die Fernverwaltung einer Private Cloud notwendig ist, kann ein VPN (Virtual Private Network) verwendet werden. Um die Sicherheitseigenschaften von VPNs zu bewerten, analysiert diese Dissertation IPsec (Internet Protocol Security), eine der wichtigsten VPN-Protokollsuiten. Für den Schlüsselaustausch in IPsec wird das Protokoll IKE (Internet Key Exchange) verwendet. IKE existiert in zwei Versionen, jede mit unterschiedlichen Modi, verschiedenen Phasen, mehreren Authentifizierungsmethoden und Konfigurationsoptionen. In dieser Dissertation wird gezeigt, dass die Wiederverwendung eines Schlüsselpaares über verschiedene Versionen und Modi von IKE hinweg zu protokollübergreifenden Authentifizierungsbypässen führen kann, die die Impersonation eines Opfers ermöglichen. Startpunkt ist die Entdeckung von Bleichenbacher-Orakeln in einem IKEv1-Modus, in dem mit RSA verschlüsselte Noncen zur Authentifizierung verwendet werden. Mit Hilfe dieser Schwachstelle brechen wir die auf RSA-*Verschlüsselung* basierenden Modi. Zusätzlich brechen wir die *signaturbasierte* Authentifizierung mit RSA sowohl in IKEv1 als auch in IKEv2. Die Bleichenbacher-Orakel existierten in den IKEv1 Implementierungen von Cisco, Huawei, Clavister und ZyXEL. Alle Anbieter haben als Reaktion auf unsere Berichte Patches veröffentlicht oder die betroffene Authentifizierungsmethode aus den Firmwares ihrer Geräte entfernt.

Eine der Möglichkeiten, Benutzerdaten sowohl in privaten als auch in öffentlichen Cloud-Infrastrukturen zu schützen, ist die client-seitige Verschlüsselung direkt vor dem Speichern in der Cloud. Wenn die Kryptographie so nah wie möglich am Benutzer stattfindet, idealerweise im Web Browser des Benutzers, ist es möglich, die Produktivitätsvorteile eines Cloud-Dienstes mit kryptographischer Sicherheit zu kombinieren. Diese Dissertation schlägt ein solches System – einen sicheren kollaborativen Echtzeit-Editor – vor. Anstatt der Cloud Dokumente im Klartext zu senden, können die Nutzer gemeinsam an verschlüsselten Dokumenten arbeiten. Dabei ist das vorgestellte System das erste Werkzeug, das eine neuartige Kombination von baumbasierten OT (Operational Transforms) Algorithmen mit einer strukturerhaltenden Verschlüsselung enthält. Es benötigt nur einen modernen Web Browser ohne zusätzliche Softwareinstallation oder Erweiterungen. Wir zeigen, dass der Speicherbedarf unseres Ansatzes im Vergleich zu allen bisherigen Ansätzen dreimal geringer ist.