Compliance-Risiken in Unternehmensnetzen minimieren

Ein Leitfaden für Unternehmen nach der EuGH Entscheidung

C 311/18 vom 16.7.2020 („Schrems II")

Dr. Eric Heitzer[1]

Übersicht

---

* Der Autor ist als Chief-Compliance-Officer und zertifizierter Datenschutzbeauftragter für rund 30 Unternehmen in Europa tätig. Von 1998-2010 verantwortete er in der Geschäftsleitung namhafter Telekommunikationsunternehmen die Bereiche Regulatory Affairs und Public Policy.

Executive Summary

- Aus Effizienz- und Komplexitätsgründen setzen Unternehmen & öffentliche Einrichtungen zunehmend auf Software-Defined Networking-Lösungen (SDN), um ihre Netze zu verwalten.

- Meist wird hierzu das Netzwerkmanagement in die Cloud eines Lösungsanbieters oder zu einem IT-Systemhaus ausgelagert, wodurch sich zum Schutz der personenbezogenen Daten betroffener Mitarbeiter, Nutzer und Geschäftspartner neue Compliance-Anforderungen im Kontext der Datenschutzgrundverordnung (DSGVO) ergeben.

- Ist der externe Cloud-Anbieter in einem Nicht-EU-Staat („Drittstaat") ansässig, sind datenschutzrechtlich zusätzlich die besonderen Regelungen der Art. 44-47 DSGVO zu beachten.

- Für Dienstleister in den USA gibt es seit der Entscheidung des EuGH vom 16.7.2020 („Schrems 2") keine verlässliche datenschutzrechtliche Grundlage für eine Zusammenarbeit. Dies gilt für den entfallenen Privacy-Shield, wie auch für die Standardvertragsklauseln, welche die aufgezeigten Risiken nicht beseitigen können. Damit verstößt die Realisierung SDN-basierter Unternehmensnetze durch US-amerikanische Anbieter gegen geltendes Datenschutzrecht.

- Ein Cloud-Anbieter mit Sitz und Rechenzentrum in der EU kann die Einhaltung des datenschutzrechtlichen Schutzniveaus gewährleisten. Nur so kann vor einer missbräuchlichen Nutzung der Daten maximaler Schutz erlangt werden.

- Haftbar für die DSGVO-konforme Datenverarbeitung verbleibt stets der Verantwortliche, der Auftraggeber in der EU. Er ist verpflichtet, die Einhaltung der datenschutzrechtlichen Vorgaben durch den Cloud-Anbieter zu überprüfen.

Vorwort

Als in den 1980er Jahren die Computerfirma Sun Microsystems den Slogan *„The network is the computer"* aufbrachte, wurde dies allgemein eher als eine nette Werbeaussage denn als ernstgemeinte Sicht auf die Zukunft verstanden.[2]

Vier Jahrzehnte später fließen Daten über weltumspannende Netzwerke mit zahllosen Verteilknoten bis hinunter zu einzelnen Standorten mit ihren lokalen Netzwerkkomponenten. Die Verfügbarkeit von Daten verbunden mit internetbasierten Kommunikationsmöglichkeiten hat die Dezentralisierung der Standorte von Konzernen wie auch Trägern der öffentlichen Hand begünstigt. Cloud-Lösungen spielen dabei eine immer wichtigere Rolle.[3] Verstärkt wird dieser Trend aktuell durch die Corona-Pandemie und einen vermutlich nachhaltigen Trend zur Einbindung von Home-Offices.[4]

Gleichzeitig sind die Serverinfrastrukturen - ganz gleich, ob in eigenen Rechenzentren (on premises) oder in der Cloud - längst durchgehend virtualisiert: Virtuelle Server bis hin zu SaaS (Software-as-a- service), virtueller Storage und - folgerichtig - virtuelle Netzwerke.

Allerdings machen die Komplexität der gestellten Aufgaben, erforderliche schnelle Reaktionszeiten und ein Mangel an qualifiziertem Personal eine effiziente, optimierte manuelle Administration auf der lokalen Netzwerkebene bis hinunter zu einzelnen Endgeräten wie Gateways, Routern, Switches oder WLAN-Access Points nahezu unmöglich.

Als Antwort darauf wurde u. a. an der Stanford University ein neuer Ansatz für Computernetze entwickelt: Software-Defined Networking (SDN). Das Konzept sieht eine Trennung / Abstrahierung der Netzwerkkomponenten Hardware und Software in eine „Data Plane" und eine „Control Plane" vor. Die i. d. R. Cloud-basierte Control Plane übernimmt Steuerung und Monitoring. Sie hat

---

[2] Der Slogan entstand 1984 und geht auf John Cage, den früheren VP und Head of Science Office bei Sun-Microsystems Mitarbeiter zurück. Zu dieser Zeit erforderte der Betrieb eines Netzwerks Vereinbarungen und Zahlungen an die Betreiber nicht interoperabler Netzwerke, z.B. für IBM Mainframes, Novell PC-Netware. Sun promotete offene Schnittstellen wie TCP/IP und Ethernet, rüstete seine Computer entsprechend aus und wurde so zum Wegbereiter für Interoperabilität. Vgl. zum Ansatz das Interview mit John Cage v. 11.7.2019, abrufbar unter: https://blog.cloudflare.com/john-gage/

[3] Einer IDC-Studie zur Folge beabsichtigen 21% Prozent aller Organisationen weltweit zusätzliche IT-Anforderungen in Public-Cloud-Umgebungen zu lösen, vgl. IDC, „COVID-19 Impact Survey, Wave 5", 2020.

[4] Der Anteil von Angestellten, die Home-Office nutzen, ist einer Studie von CISCO zufolge seit Beginn der Pandemie weltweit um den Faktor 4,7 gestiegen, vgl. H

den Überblick über die gewünschten Datenverbindungen, Bandbreiten, Zugriffsberechtigungen, Quality of Service, etc. Der Transport der Nutzdaten geschieht davon getrennt über die Data Plane.

Das Potenzial der neuen Technologie ist enorm: Ausgehend von einem Umsatz von 371,4 Milliarden € im Jahr 2020 prognostizieren *Markets&Markets* jährliche Wachstumsraten von 17,5 Prozent resultierend in einem Gesamtmarktvolumen von 832 Milliarden $ im Jahr 2025 [5]. Der Wachstumspfad setzt allerdings voraus, dass die gestiegenen Anforderungen an Sicherheit, Compliance und hier insbesondere Datenschutz bewältigt werden können.

Die vorliegende Studie arbeitet heraus, wie SDN-Lösungen im Einklang mit datenschutzrechtlichen Compliance-Anforderungen realisiert werden können. Vertiefende Informationen zu den teils komplexen technischen Zusammenhängen und Begrifflichkeiten sind einem umfangreichen Glossar mit weiteren Fundstellen zu entnehmen.

1. Software-Defined Networking: Die Ausgangssituation[6]

Software-Defined Networking (SDN) ermöglicht die zentrale, weitgehend automatisierte Konfiguration und Steuerung ganzer Netzwerkinfrastrukturen. Mit dem implementierten gemeinsamen SDN-Control-Layer werden das gesamte Netz bzw. eine Mehrzahl von Netzen und – abhängig von der Leistungsfähigkeit der Lösung – alle Geräte (Router, Gateways, Switches, WLAN Access Points) einheitlich gemanagt, und zwar unabhängig von der Komplexität der zugrundeliegenden Netztechnologie.