INTEGRITY.
Gesellschaft für Datenschutz, Geldwäscheprävention und Compliance

Minimizing compliance risks in corporate networks

A guide for companies after the European Court of Justice (ECJ) decision C 311/18 of 16.7.2020 ("Schrems II")

Dr. Eric Heitzer[1]

Overview

[*] The author holds the position of a (Chief-) Compliance Officer and Certified Data Protection Officer for around 30 companies in Europe. From 1998-2010, he was responsible for regulatory affairs and public policy in the management of well-known telecommunications companies.

Executive Summary

- For reasons of efficiency and complexity, companies and public institutions are increasingly turning to software-defined networking (SDN) solutions to manage their networks.

- In most cases, network management is outsourced to the cloud of a solution provider or to an IT system house, which results in new compliance requirements in the context of the General Data Protection Regulation (GDPR) to protect the personal data of affected employees, users and business partners.

- If the external cloud provider is located in a non-EU country ("third country"), the special regulations of Art. 44-47 GDPR must be observed in addition.

- For service providers in the USA, there has been no reliable basis under data protection law for cooperation since the decision of the ECJ of July 16, 2020 ("Schrems 2"). This applies to the no longer valid Privacy Shield as well as to the standard contractual clauses, which cannot eliminate the risks identified. Thus, the realization of SDN-based corporate networks by US providers violates applicable data protection law.

- A cloud provider with its headquarters and data center in the EU can ensure compliance with the level of protection under data protection law. This is the only way to obtain maximum protection against misuse of the data.

- Legally, the EU based controller remains the responsible and is always held liable for GDPR-compliant data processing. The controller is obliged to check the cloud provider's compliance with all data protection requirements.

Foreword

When the computer company Sun Microsystems came up with the slogan "*The network is the computer*" in the 1980s, this was widely understood to be a nice advertising statement rather than a serious look into the future.[2]

Four decades later, data flows across global networks with countless distribution nodes down to individual sites with their local network components. The availability of data combined with Internet-based communication options has favored the decentralization of corporations as well as of public entities. Cloud solutions are playing an increasingly important role in this.[3] This trend is currently being reinforced by the Corona pandemic and a presumably sustained trend towards the integration of home offices.[4]

At the same time, server infrastructures - whether in the company's own data centers (on premises) or in the cloud - have long been virtualized throughout: Virtual servers up to SaaS (software-as-a-service), virtual storage and - consequently - virtual networks.

However, the complexity of the tasks involved, the need for fast response times and a lack of qualified personnel make efficient, optimized manual administration at the local network level down to individual end devices such as gateways, routers, switches or WLAN access points virtually impossible.

In response to this, a new approach for computer networks was developed at Stanford University, among others: Software-Defined Networking (SDN). The concept provides for a separation / abstraction of the network components hardware and software into a "data plane" and a "control plane". The control plane, which is usually cloud-based, takes over control and monitoring. It has an overview of the desired data connections, bandwidths, access authorizations, quality of service, etc. The transport of user data is handled separately via the data plane.

[2] The slogan originated in 1984 and can be traced back to John Cage, former VP and Head of Science Office at Sun-Microsystems employees. At that time, running a network required agreements and payments to operators of non-interoperable networks, e.g., IBM mainframes, Novell PC-Netware. Sun promoted open interfaces such as TCP/IP and Ethernet, equipped its computers accordingly and thus became a pioneer for interoperability. Cf. on the approach the interview with John Cage v. July 11, 2019, available at: https://blog.cloudflare.com/john-gage/

[3] According to an IDC study, 21% of all organizations worldwide intend to solve additional IT requirements in public cloud environments, see IDC, "COVID-19 Impact Survey, Wave 5," 2020.

[4] The proportion of employees using home offices has increased by a factor of 4.7 worldwide since the start of the pandemic, according to a study by CISCO, cf. H

The potential of the new technology is enormous: Based on sales of €371.4 billion in the year 2020, *Markets&Markets* forecast annual growth rates of 17.5 percent resulting in a total market volume of $832 billion in 2025. However, the growth path presupposes that the increased requirements for security, compliance and in particular data protection can be managed.

This study looks at how SDN solutions can be implemented in line with data protection compliance requirements. More detailed information on sometimes complex technical context and terminology can be found in an extensive glossary with additional references.

1. Software-Defined Networking: the starting point

Software-Defined Networking (SDN) enables the centralized, largely automated configuration and control of entire network infrastructures. With the implemented common SDN control layer, the entire network or a plurality of networks and - depending on the performance of the solution - all devices (routers, ga-teways, switches, WLAN access points) are managed uniformly, regardless of the complexity of the underlying network technology.

The CONTROL PLANE is offered by almost all providers as a (public) cloud service from an external data center. Networks can thus be programmed across the board without significant implementation effort, they can be adapted to customer needs, and enable the rapid introduction of new services. With such a public cloud service, providers also address the shortage of skilled personnel among user companies and institutions that want to benefit from the advantages of SDN technology.