
Circle Networks
Grenzverschiebung
Wie SDN der Sicherheit
für Verschlusssachen dienen kann

Grenzverschiebung — wie SDN der Sicherheit für Verschlusssachen dienen kann

Software-Defined Networking (SDN) — Virtualisierung der Infrastruktur

Anwendungen in großen, standortübergreifenden Netzwerken (**SD-WAN**)

Clouds — privat, drittbetrieben oder öffentlich

Aktuelle Sicherheitsmaßnahmen für Verschlusssachen — produktbasiert und infrastrukturbezogen

Grenzverschiebung — Folgen und Möglichkeiten von SDN für Sicherheit ohne feste Infrastruktur, kurzfristig und in weiterer Zukunft…

Klassische IT-Sicherheitskonzepte setzen auf Produkte an der Grenze der Infrastruktur

Verschlusssachenanweisung (VSA) für die öffentliche Hand und Geheimschutzhandbuch (GHB) für die Privatwirtschaft

Fokus auf **Vertraulichkeit**
Keine Erwähnung von Integrität oder Verfügbarkeit

Forderungen nach **Produkten** mit Sicherheitsfunktion

Sicherheitsgateways und PAP-Strukturen — **Perimeterabsicherung**

Mittelalterlicher Ansatz —
aktuellen Nutzungsanforderungen und Gefährdungen nicht gewachsen

Das aktuelle Modell ist komplex und Komplexität ist ein Problem — für Effizienz und für die Sicherheit

Kombination zweier Paketfiltern und eines Application-Layer Gateways zum Sicherheitsgateway

Sicherung auf **Anwendungsschicht** 7 zwischen Filtern auf **Vermittlungsschicht** 3

Verhinderung effektiver Kontrolle durch sichere Protokolle (vor allem HTTPS) — **gegenseitige Behinderung** von Sicherheitsmaßnahmen

Größere Angriffsfläche mit jedem Sicherheitsprodukt

“...the optimization of each layer has to be done separately (...) in conflict with efficient implementation of data manipulation functions.

One could accuse the layered model (e.g., TCP/IP and ISO OSI) of causing this conflict.”

RFC 3439

SDN bereitet Sorgen, da es nicht ins Konzept passt — ist daher aber auch die Chance, alte Probleme zu lösen

Sicherheitsfunktionen verteilt auf verschiedene Produkte

Örtlich und zeitlich **beweglicher Perimeter** —
Hardware nicht nach roten und schwarzen Netzwerken einteilbar

Sicherung des **Informationsraums** anstatt des Netzwerks

Systemlösungen ohne einzelne, autarke Produkte

Betrachtung im Verbund notwendig

BSI-Studie ‚SDN-Produkte im Kontext von VS-IT-Systemen' (SoVIT) hat keine grundsätzlichen Probleme gefunden

Gesamtbetrachtung von SDN und VS im Allgemeinen, VS-NfD im Besonderen — Grundlagen, Markt, Einsatzszenarien, Gefährdungen, Sicherheitsmaßnahmen

Unterscheidung zwischen von der Steuerungsebene abhängigem „striktem SDN" und **„losem SDN"** mit verbliebener Eigenständigkeit der Produkte auf Datenebene

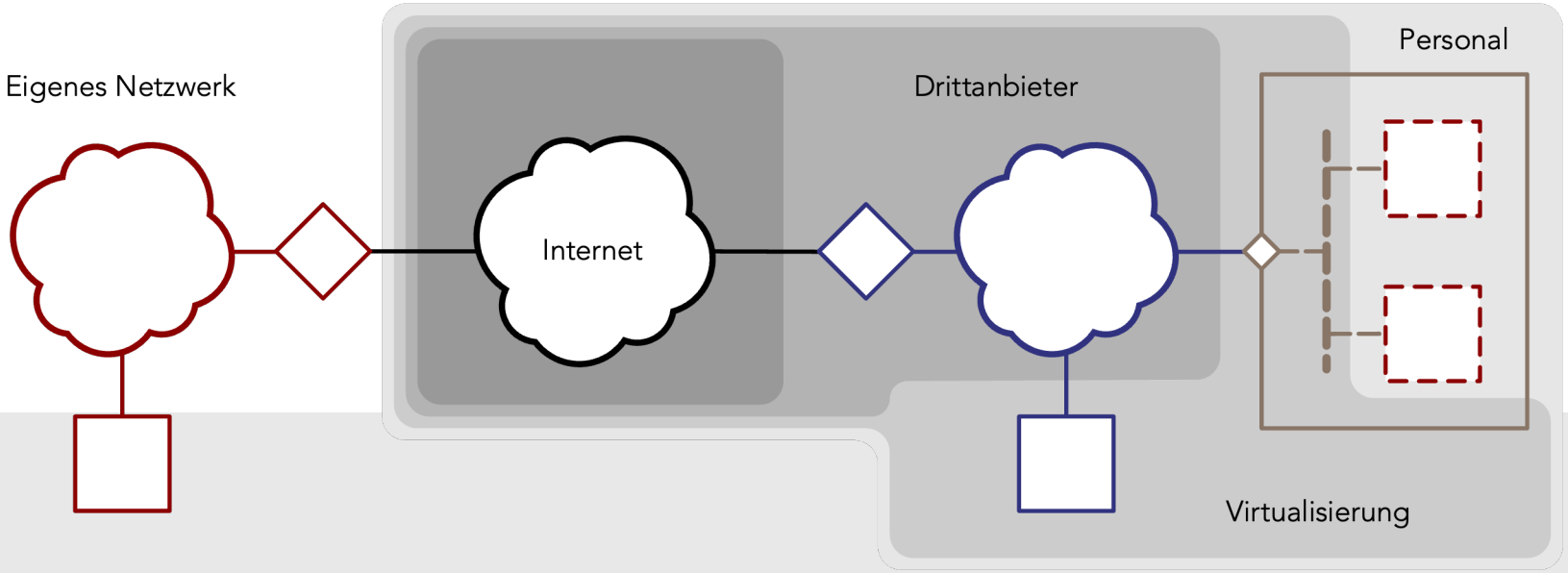
SDN-spezifische Angriffsvektoren vermeidbar oder kompensierbar

Anpassungen der Produkte notwendig — **Markteintrittsbarriere**

BSI-Studie ‚SDN-Architekturen und VS-Produkte' (SoVIT 2.0) leitet mit dem Systemansatz Anforderungen für fünf Architekturen her

Verantwortung für Sicherheit auf der **Systemebene** — funktionale **Umsetzung** durch **Produkte**

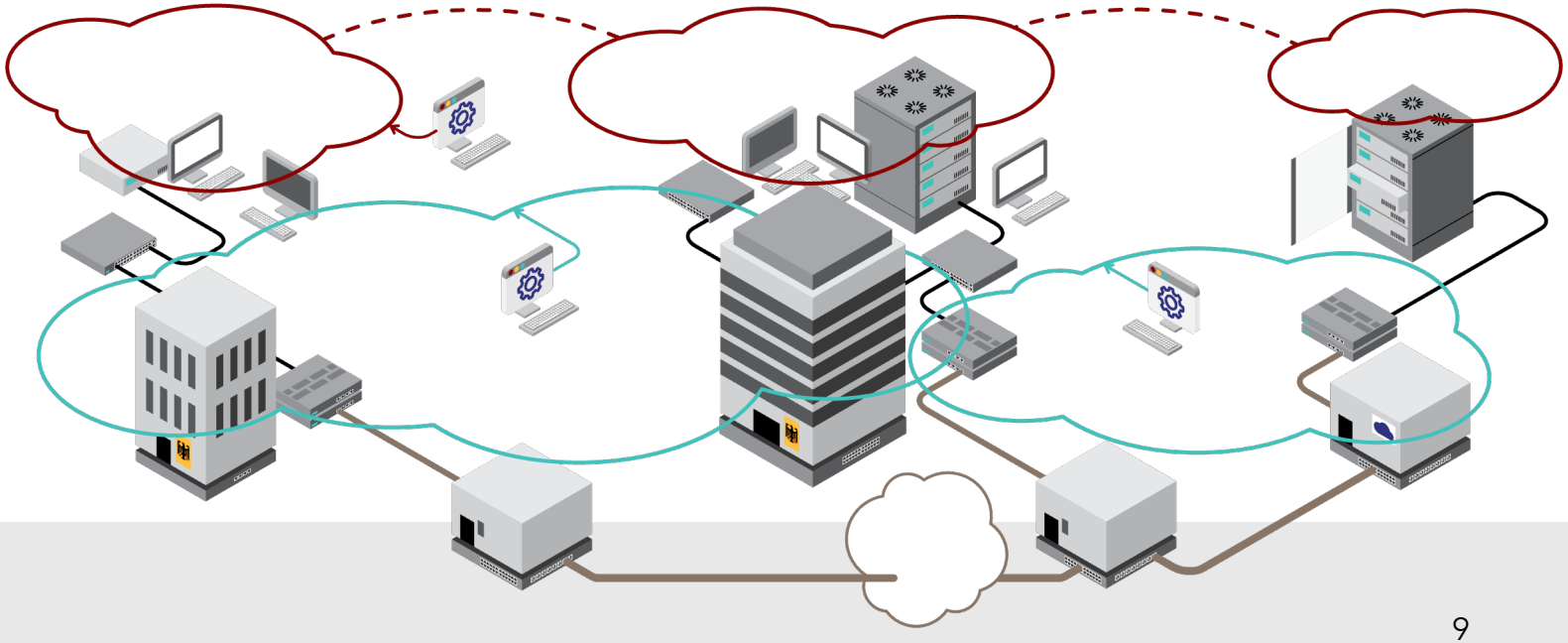
Maßnahmen an den Schnittstellen zwischen **Selbst- und Fremdbestimmung** — Extremfall öffentliche Cloud mit nichtkontrollierbarem Personal



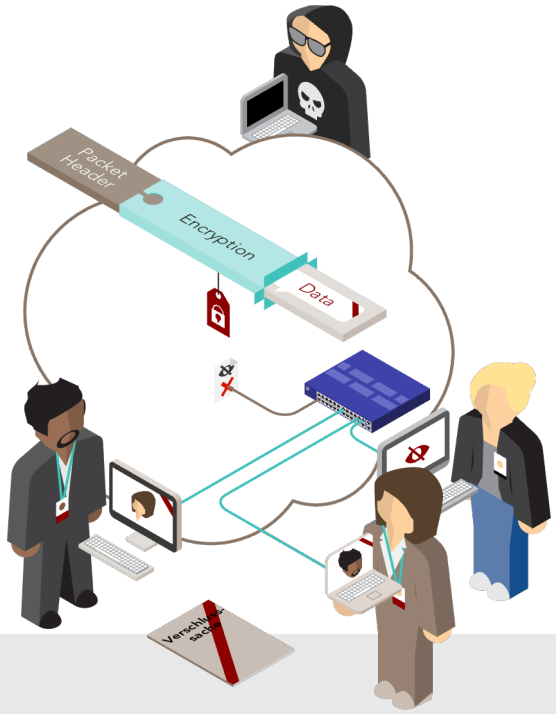
SDN verschiebt die Sicherheitsgrenze von der physischen Infrastruktur zum logischen Informationsraum

Underlay-Netzwerk als Teil der Infrastruktur nur für die Vermittlung

Rotes **Overlay-Netzwerk** als Informationsraum getrennt und abgesichert



Inhaltsbasierte Sicherheit verschiebt die Grenze weg vom Netzwerk, hin zu den Daten und Anwendungen



Konsequente Fortsetzung der Informationsraumtrennung —
Individualisierung von Einstufung und Schutz auf **Anwendungsebene**

Ende-zu-Ende-Verschlüsselung und Kennzeichnung der Daten —
Verteilung steuerbar ohne Kenntnis des Inhalts

Public-Key Infrastructure mit Teilnehmern und kaskadierten Gruppen

Clouddienste und Webkonferenzen, automatisch angepasst
an Teilnehmer und deren Rechte

SDN wird jetzt für die Informationsraumtrennung und in Zukunft für die inhaltsbasierte Sicherheit gebraucht

Infrastrukturbasierte Sicherheit nicht mehr zeitgemäß

Informationsraumbasierte Sicherheit — zeitnah erreichbar

SDN für die Maßnahmen — „aktiv“ als Verschlüsselung, „passiv“ als Sperrung

Inhaltsbasierte Sicherheit — langfristige Lösung mit minimaler Komplexität

Anwendungen und Geräte mit „aktiver“ **Rechtenerkennung**,
SDN für die „passive“ Vermittlung

Circle Networks

Fritschestraße 26
10585 Berlin

info@circle-networks.com

P250003P