Best Practises für den sicheren Betrieb von Software-definierten Netzen

Claas Lorenz [*] Nicholas Gray [†] Raphael Durner [‡] Benedikt Pfaff [§]
David Hock [¶] Thomas Zinner [‖]

7. Mai 2018

1 Einführung

Im Gegensatz zu klassischen Netzen folgen Software-definierte Netze (SDN) einem zentralisierten Netzparadigma. Grundsätzlich werden Netze in drei Schichten mit unterschiedlichen Aufgaben unterteilt:

Datenschicht Die Datenschicht leitet Netzpakete anhand einer einfachen Entscheidungsgrundlage durch das Netz.

Kontrollschicht In der Kontrollschicht wird diese Entscheidung konfiguriert und somit über die Paketflüsse im Netz entschieden.

Applikationsschicht Die Applikationsschicht ermöglicht dem Anwender die Konfiguration verschiedener, von der Kontrollschicht angebotener, Optionen.

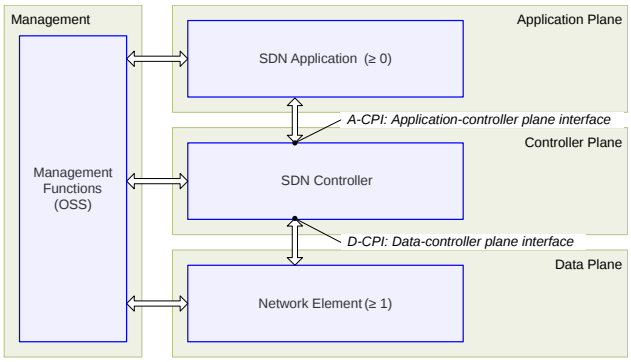

Abbildung 1: Architektur eines SDN (entnommen: [1]).

In klassischen Netzen sind Daten- und Kontrollschicht jeweils in den Netzgeräten implementiert. Die Kontrollschicht wird dabei mit verteilten Protokollen, wie beispielsweise LLDP, STP oder OSPF, umgesetzt. Im Gegensatz dazu werden, wie in Abbildung 1 dargestellt, in einem SDN die Daten- und die Kontrollschicht voneinander getrennt, sodass ein logisch zentralisierter Controller unabhängig von den Netzgeräten betrieben werden kann. Aufbauend auf diesem Controller kann mittels Applikationen die Netzfunktionalität vorgegeben und konfiguriert werden. Dabei übermittelt der Controller die Vorgaben an die Netzgeräte, welche sie in ihren Entscheidungstabellen manifestieren, anhand denen sie eingehende Netzpakete verarbeiten. Mögliche Aktionen sind beispielsweise das Verwerfen, Umschreiben, Weiterleiten oder Metern des Pakets. Im Falle von Paketen, für welche es keine Tabelleneinträge gibt, kennt SDN zwei Modi:

[*] genua GmbH (Kirchheim bei München), claas_lorenz@genua.de
[†] Universität Würzburg, nicholas.gray@informatik.uni-wuerzburg.de
[‡] Technische Universität München, r.durner@tum.de
[§] Infosim GmbH, pfaff@infosim.net
[¶] Infosim GmbH, hock@infosim.net
[‖] Technische Universität Berlin, zinner@inet.tu-berlin.de

- Im *proaktiven* Modus werden Pakete verworfen.
- Im *reaktiven* Modus werden sie hingegen zur Entscheidungsfindung an den Controller gesandt.

Von der Zentralisierung der Netzkontrolle versprechen sich viele Anwender eine Reduzierung ihrer Betriebskosten (OPEX). SDN erlauben die Umsetzung einer einfachen aber flexiblen Netzvirtualisierung, sodass die bestehende Inftrastruktur besser ausgelastet werden kann. Somit muss der Netzausbau seltener durchgeführt werden, was die Investitionskosten (CAPEX) senkt. Darüber hinaus kann das Netz mit günstiger Standardhardware bestückt werden, was sich ebenfalls positiv auf die Höhe der Investitionen auswirkt.

Im folgenden Abschnitt 2 werden zunächst die generellen Angriffsszenarien in SDN vorgestellt und bewertet. Anschließend werden in Abschnitt 3 passende Gegenmaßnahmen vorgestellt.

2 Sicherheitsanalyse

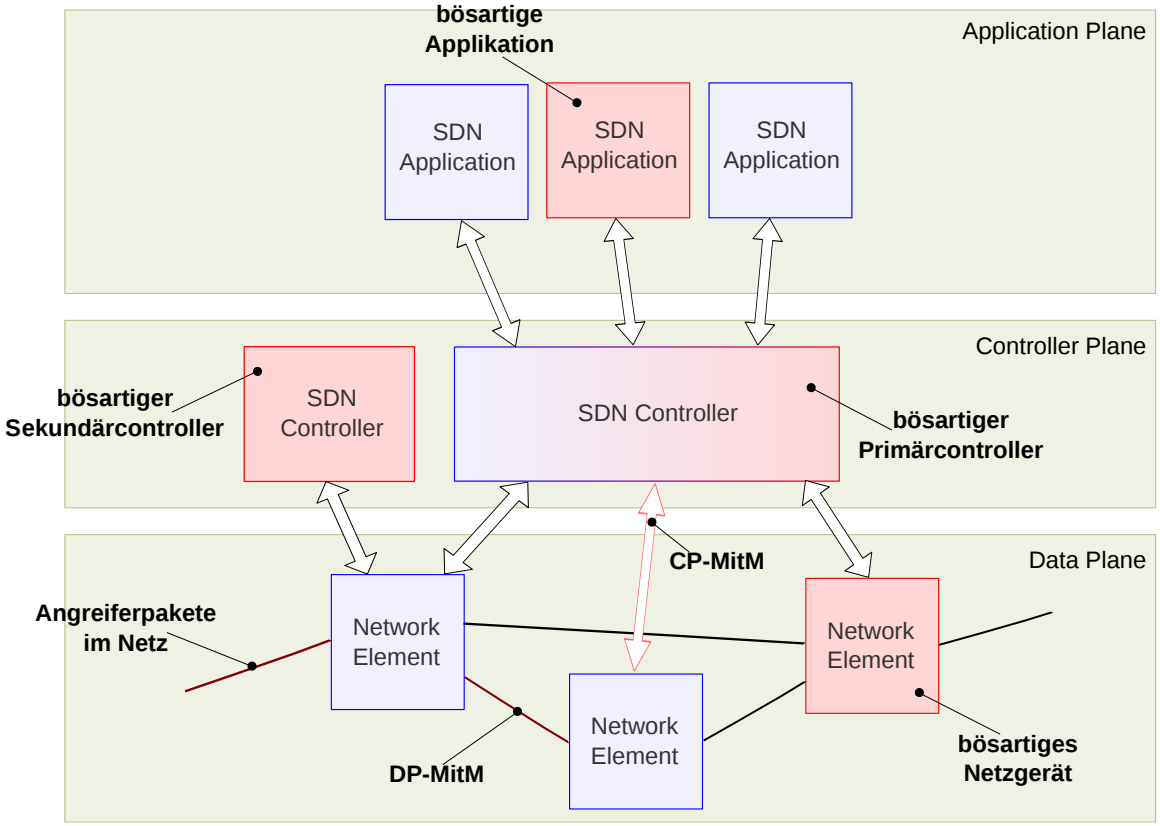

Abbildung 2: Mögliche Angriffsvektoren in einem SDN.

Wie in Abbildung 2 dargestellt, bietet ein SDN zahlreiche Angriffsvektoren. Allerdings sind diese nicht unbedingt spezifisch für SDN sondern treten auch in klassischen Netzen wie in Tabelle 1 gelistet auf. Insbesonders die Angriffe in der Datenschicht stellen keine Besonderheit von SDN dar. Entsprechende Gegenmaßnahmen, wie beispielsweise physische Zugriffsbeschränkungen oder Perimeterfirewalls, können grundsätzlich auch in SDN eingesetzt werden. Eine Weiterentwicklung von Firewalls bezüglich der besseren Nutzung der

Angriffsvektor	**Schicht**	**SDN-spezifisch?**	**Auswirkungen**
Angreiferpakete im Netz	DP	✗	Angriffe auf Netzgeräte, DoS
DP-MitM	DP	✗	Manipulation div. Flows, Angriffe auf Netzgeräte, DoS
Bösartiges Netzgerät	DP	✗	Manipulation div. Flows
CP-MitM	CP	✓	Manipulation div. Flows und des Controllers
Bösartiger Primärcontroller	CP	✓	Manipulation des Netzes
Bösartiger Sekundärcontroller	CP	✓	Manipulation eines Teilnetzes
Bösartige Applikation	AP	✓	Manipulation des Netzes gemäß Controller-API

Tabelle 1: Angriffsvektoren im SDN und Auswirkungen auf die Sicherheit des Netzbetriebs

Möglichkeiten von SDN ist jedoch anzuraten um den Betrieb zu vereinfachen und gegebenfalls eine hinreichende Skalierbarkeit der Sicherheitslösung zu erreichen (siehe auch [2]). Angriffe innerhalb der Datenschicht treten insbesonders dann auf, wenn der Angreifer die Kontrolle über einen direkten Netzteilnehmer inne hat. Dies ist beispielsweise bei einem infizierten Host oder einer gemieteten virtuellen Maschine in einem Rechenzentrum der Fall.

Spezifische Angriffsvektoren in SDN treten mit der Trennung von Daten- und Kontrollschicht sowie der logischen Zentralisierung letzterer auf. Ein Angreifer mit Kontrolle auf den Kommunikationskanal (CP-MitM) zwischen Netzgerät und Controller kann die Kontrollnachrichten beliebig manipulieren, diese verwerfen oder eigene Nachrichten einbringen und somit direkt die Einträge in den Entscheidungstabellen bestimmen. Hat der Angreifer Zugriff auf eine hinreichende Anzahl von Kontrollverbindungen, kann er beliebige Datenflüsse verwerfen, umleiten oder verstecken, ohne dass der Operator dies feststellen kann. Dieses Angriffszenario ist insbesonders dann realistisch, wenn das Kontrollnetz in-band, also direkt auf der Produktivinfrastruktur, läuft und der Angreifer fähig ist dort Man-in-the-Middle zu werden. Für einfache Störungen des SDN reicht es jedoch schon, wenn der Angreifer Pakete in den Kontrollkanal schicken kann.

Darüber hinaus gehen Szenarien, in welchen der Angreifer den Controller übernommen hat und somit beliebig das gesamte Netz manipulieren kann. Eine Detektion ist ohne externe Maßnahmen nicht möglich, während die Auswirkungen eines erfolgreichen Angriffs verheerend sein kann. Die logische Zentralisierung des Controllers stellt folglich die größte sicherheitliche Herausforderung dar. Ein gangbarer, aber herausfordernder, Angriffsweg besteht, wenn der Angreifer in der Lage ist, eine Sicherheitslücke in der Controller-Software auszunutzen indem er Angriffspakete zum Controller schickt. Alternativ ist dieser Angriff trivial, wenn dem Angreifer eine Infektion des Hostsystems gelingt, auf welchem der Controller läuft.

Ebenfalls kritisch ist das Einschleusen eines Zweitcontrollers ins Netz durch einen Angreifer. Das SDN-Paradigma erlaubt ein Aufsetzen der Kontrollschicht als verteiltes System mit mehreren, zusammenarbeitenden Controller-Instanzen. Zweitcontroller werden dabei genutzt um dem Netz per Redundanz einen gewissen Grad an Ausfallsicherheit zu ermöglichen. Angreifer mit Zugriff auf einen solchen Controller können Teile des oder sogar das gesamte Netz darüber kontrollieren. Um diesen Angriff durchführen zu können, muss der Angreifer stabil mit dem Netzgerät kommunizieren können. Dies ist beispielsweise gegeben, wenn er Zugriff auf einen infizierten Host im selben Netz hat, in welchem die Kontrollschnittstelle des Netzgeräts zugreifbar ist. Im Falle eines In-Band-Kontrollnetzes wäre dies zugleich das Produktivnetz und manche Netzgeräte erlauben Kontrollverbindungen auf allen Interfaces.

Hat ein Angreifer die Kontrolle über eine SDN-Applikation kann er das Netz gemäß der, vom Controller

bereitgestellten, API gesteuert werden. Übliche Controller bieten eine (REST-)API zur direkten Manipulation von Entscheidungstabellen in den Netzgeräten, womit die Auswirkungen ähnlich weitreichend sind wie bei einem kompromittierten Controller. Gangbar ist dieser Angriff insbesonders, wenn Applikationen von Drittanbietern über einen App-Store mit mäßigen Qualitätsstandards bezogen werden. Aber auch eine Infektion des Hosts, auf welchem die Applikation läuft, ermöglich eine triviale Durchführung dieses Angriffes. Allerdings können Eingriffe mittels SDN-Applikationen nicht einfach versteckt werden, weil die API-Zugriffe typischerweise in Logs des Controllers registriert werden. Außerdem können Unregelmäßigkeiten gegebenenfalls durch andere Applikationen erkannt und gemeldet werden, weil alle Applikationen die selbe Sicht auf den Netzzustand erlangen und diesen gegen bestehende Policies prüfen können. Dass übliche Applikationen bereits Gegenmaßnahmen dieser Art implementieren, ist eher ungewöhnlich und zur Zeit noch experimentelle Forschung. Daher werden im folgenden Abschnitt auf Maßnahmen vorgestellt, die bereits mit üblichen Netzgeräten und Controllern umgesetzt werden können.

3 Maßnahmen

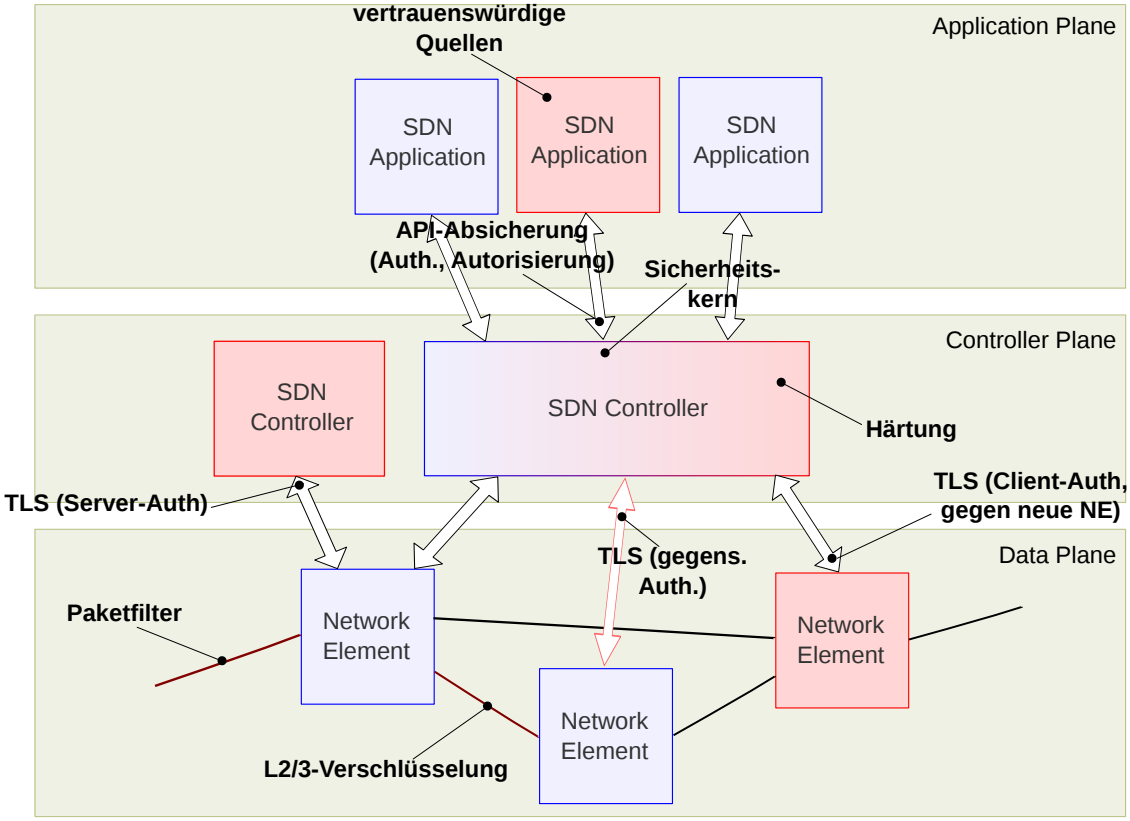

Abbildung 3: Mögliche Gegenmaßnahmen für Angriffe in einem SDN.

Bevor man über geeignete Maßnahmen gegen die oben angeführten Angriffsszenarien nachdenkt, steht eine Analyse der eigenen Betriebsziele sowie deren Umsetzung mittels SDN. Generell ist es für die Sicherheit förderlich, wenn Komplexität vermieden wird. So werden nicht nur die konkreten Angriffsvektoren reduziert,

die sich durch große Softwareinstallation und komplizierte Konfigurationen ergeben, sondern potenziell auch die Operationskosten gering gehalten.

Ausgehend von den Anforderungen an die Funktionen des Netzes sowie deren Betrieb, sollte geprüft werden, ob man auf einen reaktiven Betrieb des SDN verzichten und stattdessen eine proaktive Konfiguration nutzen kann (z.B. mit [3]). Diese Maßnahme verbessert signifikant die Trennung zwischen den Netzgeräten in der Datenschicht und dem verwundbaren Controller. Um in diesem Szenario Angriffspakete zum Controller schicken zu können, muss der Angreifer die volle Kontrolle über ein Netzgerät haben, was bereits ein fortgeschritteneres Angriffsszenario darstellt. Eine weitere Herausforderung beim reaktiven Modus besteht darin, dass durch das Lernen des Netzzustandes auch gezielt manipulierte Informationen einfließen können. Beispielsweise kann ein Angreifer LLDP- oder ARP-Nachrichten fälschen. Dies ist zwar auch in klassischen Netzen möglich, aber in einem SDN ist potenziell das gesamte Netz betroffen.

Wenn reaktives Verhalten für bestimmte Netzfunktionen benötigt wird, sollte man prüfen inwiefern man dieses Verhalten über eigene Regeln im Netzgerät auf bestimmte Paketflüsse begrenzen kann. So wird die Angriffsoberfläche weiterhin minimal gehalten. Ein weiterer Vorteil des proaktiven Modus ist der geringe Resourcenbedarf für den Controller. Da dieser nur eine geringe Menge an SDN-Protokollverkehr bewältigen muss und keinen Denial-of-Service Angriffen aus der Datenschicht ausgesetzt ist.

Eine weitere allgemeine Sicherheitsmaßnahme besteht im Betrieb eines separaten Netzes für den Kontroll- und Managementverkehr. Dies stellt sicher, dass ein Angreifer in der Datenschicht keine Man-in-the-Middle-Attacken gegen die Kontrollverbindungen durchführen kann. Die Kehrseite dieses Ansatzes sind die notwendigen Investitionen und Operationskosten für ein solches separates Netz. Auch hier gilt die Maßgabe, das Netz möglichst einfach zu halten, sodass die Kosten im Rahmen bleiben. Im Vergleich zum Produktivnetz hat das Kontroll- und Managementnetz eher moderate Performanzanforderungen und kann daher gut als klassisches Netz oder als einfaches In-Band-SDN aufgesetzt werden.

Im Folgenden werden nun die, in Abbildung 3 dargestellten, Maßnahmen vorgestellt, die unabhängig vom gewählten Betriebsmodus oder der Verwendung eines separaten Kontroll- und Managementnetzes genutzt werden können.

Angreiferpakete im Netz Gegen ein Eindringen von Pakten, die durch einen Angreifer kontrolliert werden, hilft nur das klassische Konzept der Paketfilterung, der diese Pakete frühzeitig erkennt und verwirft. Klassische Perimeterfirewalls setzen dieses Konzept um und auch Softwarefirewalls können in virtualisierenden Infrastrukturen, wie sie beispielsweise in Cloud-Rechenzentren zu finden sind, für diese Aufgabe genutzt werden. Cloudmanagementsysteme, wie beispielsweise OpenStack (vgl. [4]), legen beim Start von virtuellen Maschinen Regeln an, welche die Kommunikation eines potenziellen Angreifer in einer solchen virtuellen Instanz stark einschränken. Dadurch werden wirkungsvolle Angriffe dieser Art massiv erschwert. SDN bietet grundsätzlich hinreichende Primitive zur Verkehrsfilterung. So erlaubt beispielsweise OpenStack Neutron die Nutzung des Open vSwitch im Hypervisor zur Durchsetzung solcher Filterregeln.

Datenschicht MitM Diese Art von Angriffen sind nur sehr schwer zu detektieren, weil der Angreifer in der Lage ist sämtlichen Verkehr zu fälschen. Die wirkungsvollste Gegenmaßnahme stellt folglich eine Verschlüsselung des Verkehrs in der Datenschicht (z.B. mittels IPSec) dar. Dies erhöht jedoch die Komplexität des Netzes und damit die operativen Kosten.

Eine denkbare Gegenmaßnahme besteht in einer strengen Umsetzung von Portsicherheit beispielsweise mittels 802.1X (vgl. [5]). Alternativ können die praktischen MitM-Angriffe ARP- sowie DHCP-Spoofing angegangen werden, wenn Anfragen durch den Controller oder eine entsprechende Netzfunktion zentralisiert beantwortet werden. Hier können anhand von Netztopologie und Routinginformationen geeignete Filter zur Angriffsmitigation implementiert werden. Dieser Ansatz ist jedoch eher als experimentell einzustufen und auch fortgeschrittene Controller wie ONOS mit seinem Neighbor-Resolution-Service (vgl. [6]) setzen diese Maßnahme zur Zeit nicht um.

Bösartiges Netzgerät Wenn ein Netzgerät erst einmal infiziert ist, kann der Betreiber nur wenig tun um negative Auswirkungen auf das Netz zu verhindern. Lediglich das Einbringen neuer beziehungsweise gefälschter Netzgeräte durch den Angreifer kann erkannt und deren logische Einbindung ins Netz unterbunden werden, wenn für den Kontrollkanal TLS mit Clientauthentifizierung genutzt wird. Netzgeräte, die sich nicht ausreichend authentifizieren können, werden dann vom Controller nicht akzeptiert, nicht mit Traffic versorgt und bleiben somit isoliert. Generell ist die Nutzung von TLS im Kontrollkanal auch als Maßnahme gegen andere Angriffe in der Kontrollschicht sinnvoll, insbesonders wenn kein separates Kontrollnetz betrieben wird.

Falls die verwendeten Netzgeräte kein TLS unterstützen, kann auf die experimentelle Methodik des Device-Fingerprintings (vgl. [7]) zurück gegriffen werden. Dafür werden im Controller zunächst Profile der verwendeten Netzgeräte gelernt. Im eigentlichen Betrieb wird für jedes neue Gerät ein Fingerprint erstellt und mit den bekannten Profilen verglichen. Geräte, die diesen Test nicht bestehen, werden vom Controller nicht akzeptiert und können somit nicht am Betrieb teilnehmen. Diese Methodik ist als experimentell einzustufen und ist noch nicht im Lieferumfang gängiger Controller enthalten.

Kontrollschicht MitM Eine Man-in-the-Middle-Attacke gegen die Kontrolverbindungen kann ebenfalls nur mit TLS und gegenseitiger Authentifizierung effektiv und gefahrfrei verhindert werden. Dadurch wird vermieden, dass Netzgerät oder Controller durch den Angreifer impersonifiziert werden können und die Verschlüsselung schützt den Kontrollverkehr vor Manipulationen, sodass die Integrität des Kontrollprotokolls uneingeschränkt gegeben ist.

Alternativ ist auch der Einsatz eines virtuellen Netzes für den Kontrollverkehr denkbar. Hier ist allerdings die Gefahr von Konfigurationsfehlern groß, die im schlimmsten Fall zum Verlust der Konnektivität zwischen Netzgerät und Controller führt. Die Wiederherstellung eines produktiven Zustands ist dann nur noch manuell möglich. Das Netz ist in dieser Zeit nicht oder nur sehr eingeschränkt produktiv nutzbar.

Bösartiger Primärcontroller Eine Kompromittierung des zentralisierten Controllers stellt den mächtigsten Angriff in einem SDN dar. Daher ist bei der Auswahl und dem Betrieb des Controllers auf eine hohe Qualität der Implementierung sowie eine sichere und gehärtete Laufzeitumgebung zu achten. Auch hier greift die allgemeine Empfehlung Komplexität zu vermeiden, sodass dieses kritische System mit vertretbarem Aufwand überwacht und, im Falle eines erkannten Angriffs, durch ein Backupsystem ersetzt werden kann.

Bösartiger Zweitcontroller Gegen diese Art von Angriff hilft der Einsatz von TLS mit Serverauthentifizierung. Ein Controller, der sich nicht mittels eines vorkonfigurierten Zertifikats ausweisen kann, wird vom Netzgerät nicht akzeptiert. Zusätzlich können viele Netzgeräte in einen Modus versetzt werden, in welchem sie grundsätzlich keine externen Kontrollverbindungen annehmen und stattdessen versucht sich mit einem oder mehreren konfigurierten Controllern zu verbinden. Steht diese Option zur Verfügung, sollte sie unbedingt genutzt werden.

Bösartige Applikation Um das Netz vor Angriffen mittels kompromittierten Applikationen zu schützen, sollte zunächst darauf geachtet werden nur Applikationen aus vertrauenswürdiger Quelle zu verwenden. Insbesonders bei der Verwendung von Drittanbieterapps aus einem App-Store ist eine Risikoanalyse angeraten, welche die sicherheitliche Praxis des App-Stores berücksichtigt. Flankiert werden sollte diese Maßnahme durch vertragliche Risikominimierungen sowie gegebenenfalls eine Auditierung der Applikation.

Auf technischer Ebene können je nach Güte des Controllers weitere Maßnahmen ergriffen werden. So bieten viele Controller eine REST-Schnittstelle an, welche mit herkömmlichen Maßnahmen wie beispielsweise TLS mit Clientauthentifizierung abgesichert werden kann (vgl. [8]). Darüber hinaus gehen Controller, welche einen Sicherheitskern bereitstellen, der mittels Policies konfiguriert werden kann. Beispielsweise kann so der Lese- und Schreibzugriff von Applikationen auf die Netzgeräte limitiert werden. Allerdings implementieren die gängigen Controller diese Mechanismen nicht.

4 Fazit

Dieser Leitfaden über Best-Practices für den sicheren Betrieb von Software-definierten Netzen schlägt eine Reihe von einfachen Maßnahmen gegen übliche Angriffe vor. Anhand einer systematischen Analyse werden die Problemfelder herausgearbeitet und mögliche Lösungen präsentiert. Neben zahlreichen technischen Maßnahmen ist die Einhaltung des sicherheitlichen Minimalprinzips hervorzuheben. Die dadurch erreichbare niedrige Komplexität erhöht die Sicherheit signifikant und verringert sowohl den Einsatz von operationellen Resourcen als auch die notwendigen Investitionen im Vergleich zu einer komplexen Lösung.

Über die, in diesem Leitfaden vorgestellten, Maßnahmen hinaus, gibt es zahlreiche wissenschaftliche Arbeiten zum Themenkomplex SDN-Sicherheit. Einen guten Überblick bietet dabei ein Survey aus dem Jahr 2016 (vgl. [9]). Eine Stärke von SDN ist die Flexibilität bei der Umsetzung der Kontrollschicht im zentralisierten Controller. Dies erleichtert auch die Überführung von Forschungsergebnissen in den produktiven Betrieb.

Danksagung

Dieser Leitfaden entstand im Forschungsprojektes SarDiNe und wurde im Rahmen des Programmes *KMU-Innovativ* durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert.

Literatur

[1] SDN Architecture. Technical Report ONF TR-502, Open Networking Foundation, June 2014.

[2] Claas Lorenz, David Hock, Johann Scherer, Raphael Durner, Wolfgang Kellerer, Steffen Gebert, Nicholas Gray, Thomas Zinner, and Phuoc Tran-Gia. An SDN/NFV-Enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement. *IEEE Communications Magazine*, 55(3):217–223, 2017.

[3] Faucet - Open source SDN Controller for production networks. `http://faucet.nz/`. Letzter Zugriff: 25.04.2018.

[4] `https://openstack.org/`. Letzter Zugriff: 25.04.2018.

[5] Eckhart Traber. 802.1x: Zugriffskontrolle im LAN und WLAN-Netzwerk. `https://www.tecchannel.de/a/802-1x-zugriffskontrolle-im-lan-und-wlan-netzwerk,2023084`, 2009. Letzter Zugriff: 02.05.2018.

[6] `https://wiki.onosproject.org/display/ONOS/Neighbour+Resolution+Service`. Letzter Zugriff: 02.05.2018.

[7] Nicholas Gray, Thomas Zinner, and Phuoc Tran-Gia. Enhancing SDN security by device fingerprinting. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, May 8-12, 2017*, pages 879–880, 2017.

[8] Philip Porras, Seungwon Shin, Vinod Yegneswaran, Martin W. Fong, Mabry Tyson, and Guofei Gu. A security enforcement kernel for OpenFlow networks. In *Proceedings of the first workshop on Hot topics in software defined networks, HotSDN@SIGCOMM 2012, Helsinki, Finland, August 13, 2012*, pages 121–126, 2012.

[9] Sandra Scott-Hayward, Sriram Natarajan, and Sakir Sezer. A Survey of Security in Software Defined Networks. *IEEE Communications Surveys and Tutorials*, 18(1):623–654, 2016.