КИБЕРСИГУРНОСТ НА ЕЛЕКТРОЕНЕРГИЙНИТЕ СИСТЕМИ И МРЕЖИ СЪС СОФТУЕРНО ДЕФИНИРАНА МРЕЖОВА АРХИТЕКТУРА SDN MICROSENSE – ОБЗОР И ПИЛОТНО ПРОУЧВАНЕ

инж. Тихомир Гоглев

CYBERSECURITY IN THE ELECTRICAL POWER AND ENERGY SYSTEM (EPES) WITH SOFTWARE- DEFINED NETWORK ARCHITECTURE SDN MICROSENSE – REVIEW AND PILOT

Tihomir Goglev, M.Eng.

Abstract

Software-Defined Network (SDN) is a network architecture which decouple network control and forwarding functions, enabling network control to become directly programmable. The SDN paradigm can bring new opportunities to enhance security of power grid communication and SCADA/EMS networks, offering new approaches for preventing, detecting and mitigating cyberattacks. Based on this reality, the SDN-microSENSE project intends to provide a set of secure, privacy-enabled and resilient to cyberattacks tools, thus ensuring the normal operation of EPES. During the pilot massive false data injection attack will be launched concurrently against SCADA/EMS system, that will target the data integrity. The main objective of the pilot is tovalidate the SDN microSENSE platform in the operational environment of the Bulgarian grid operator.

Увод

Цифровата инфраструктура, поддържаща електроенергийната система, играе все по-голяма и важна роля, предоставяйки нови възможности за оперативно управление и регионално сътрудничество. Информационните и комуникационни технологии, съставящи тази инфраструктура, трябва да осигуряват и гарантират конфиденциалност, интегритет, достъпност и автентичност в обмена на данни.

Софтуерно дефинирана мрежова архитектура

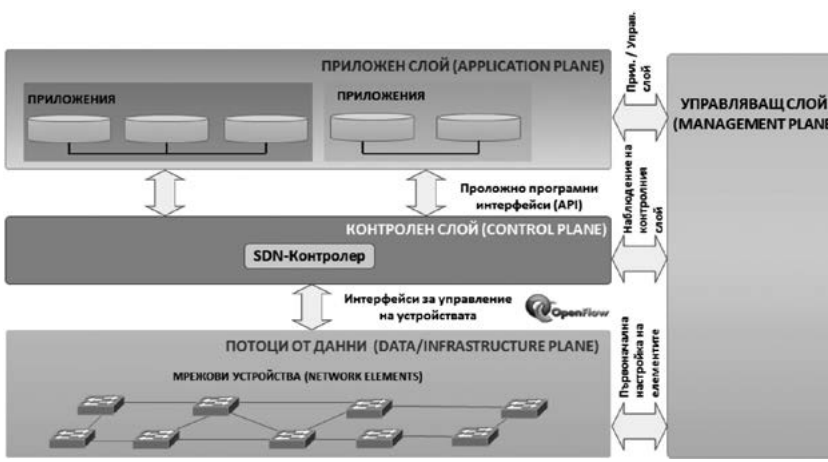
Софтуерно дефинирана мрежова архитектура или Software-Defined Network (SDN) е архитектурна концепция, при която управлението на мрежовата инфраструктура се отделя от механизмите за предаване на

данни, давайки възможност мрежовият контрол да бъде програмиран директно. При такова разделение работещите в мрежата устройства само насочват потоците от данни, без да извършват каквито и да е решения за тяхната маршрутизация и управление. Управляващата логика се измества в специален SDN контролер, чрез който централизирано могат да се задават различни политики за управление на трафика от данни или да се извършват промени в конфигурацията на мрежата. SDN не е технология, а архитектура, която отделя контролните функции на мрежата от устройствата, които пренасят данните [1].

Независимо от производителя основните компоненти на SDN решението са SDN контролер, програмируема мрежова инфраструктура и приложен слой за управление и директно програмиране на функциите на мрежовата инфраструктура. Фигура 1 изобразява логически изгледа на SDN архитектурата, като съгласно Open Network Foundation (ONF) са дефинирани следните слоеве [2]:

• Инфраструктурен слой или слой на данните - тук се разполагат всички физически мрежови устройства, позволяващи да бъдат управлявани от SDN контролер.

• Контролен слой – на това ниво функционират SDN контролерите, които посредством приложно-програмен интерфейс (Application Programming Interface – API) и протокол за комуникация OpenFlow, задават различни политики за управление на инфраструктурното ниво.



Фигура 1. Основни компоненти на **SDN** архитектурата

• Приложен слой – включва едно или повече приложения, всяко от които има специфичен контрол върху набор от ресурси, предоставени от един или повече SDN контролери

• Управляващ слой – представлява система за управление на мрежата (Network Management System – NMS).

Логическото разделение на функциите между мрежовите устройства и SDN контролера се извършва посредством приложно-програмен интерфейс (API). За да се реализира комуникацията между инфраструктурното ниво и контролерите в SDN архитектурата, се използва протоколът OpenFlow. Комутаторите, поддържащи този протокол, имат една или няколко таблици (flowtables), които съдържат набор от правила за управление на потоците от данни (dataflows). За всеки отделен поток се отнасят различни правила, които определят специфични действия за неговото обработване –препращане към съответното направление, отхвърляне или модифициране В SDN концепцията, използвания термин „поток от данни" се използва, за да означи поредица от данни, които попадат в обхвата на конкретно правило за управление, зададено в SDN контролера [3].

Киберсигурност чрез *SDN*

SDN архитектурата предоставя възможност за значително подобряване на сигурността на информационната и комуникационна инфраструктура, както и на SCADA/EMS системите, използващи тази инфраструктура. SDN контролерите имат пълна видимост върху потребителите, устройствата и приложенията в мрежата, както и способност да препрограмират инфраструктурата във всеки един момент. Това ги поставя в състояние ефективно да идентифицират и смекчават злонамерени потоци от данни, които са част от кибератака, предоставяйки на потребителя корекцията, която трябва да направи [4]. Този повсеместен поглед, комбиниран със съвременни алгоритми за машинно самообучение, изпълнявани от софтуерни компоненти, работещи в приложения слой, означава, че има много нови възможности контролерът да налага правила за сигурност върху цялата система.

Автоматично откриване и реакция със *SDN MicroSENSE*

Основната концепция на SDN MicroSENSE се състои в периодично натрупване на статистическа информация за пренасяните данни, след което в реално време се прилагат алгоритми за класификация върху тези статистически данни, с цел откриване на аномалии. Ако се открие

аномалия, приложенията работещи в приложния слой, инструктират SDN контролера кои злонамерени потоци от данни трябва да бъдат изолирани или поставени под карантина. Изолирането и ограничаването на потоци от данни, съдържащи в себе си атакуваща информация, се извършва от софтуерни компоненти, базирани на алгоритми за машинно самообучение, представляващи софтуерни работни рамки (frameworks).

Пилотно проучване

Основната цел на пилотното проучване е симулиране на защита от кибератака срещу автоматичното честотно регулиране (АЧР) на Електроенергийната систем (ЕЕС) . Изследването ще се извърши на два етапа.

Първи етап

Симулиране на масирана кибератака с подменени данни от измервания на електрически величини, извършена едновременно от няколко места - собствена подстанция, подстанция на електроразпределително дружество и два външни производителя на енергия срещу SCADA / EMS на ЕЕС. Атаката ще бъде насочена срещу интегритета на данните от измерванията.

Втори етап

Смекчаване на кибератаката с платформата SDN MicroSENSE.

Очаквани резултати

Първи етап ще покаже резултати по отношение на точност (оценка за откриване на аномалии), ефикасност (време за откриване на аномалия) и резултатност (точност при откриване истинските заплахи).

Втори етап ще валидира платформата по отношение на смекчаване на кибератаки .

Заключение

Намаляването на времето за реакция при кибератаки е от решаващо значение при защита на критична инфраструктура. Софтуерно дефинираната мрежова архитектура дава нова перспектива за защита на инфор-

мацията, улеснявайки и подобрявайки работата на свързаните с мрежата приложения за сигурност. Поради способността на SDN контролера да има пълна видимост върху устройствата и приложенията, както и способността му да препрограмира мрежовата инфраструктура във всеки един момент от времето, могат автоматично да бъдат откривани и отказвани потоци от данни, съдържащи атакуваща информация. Чрез SDN могат автоматично да бъдат изолирани и смекчавани атаки, характеризиращи се с рязко нарастващ трафичен обем, като „Разпределени атаки за отказ от обслужване (Distributed Denial of Service - DDoS), атаки по метода груба сила (brute-force intrusions), разпространение на зловреден софтуер, както и различни видове подслушващи атаки.

Библиография

[1] SDN Architecture. Open Networking Foundation. Palo Alto, CA. 2014. Accessed on: June, 2014. [online]. Available:https://www.opennetworking.org/wp-content/uploads/2013/02/TR_SDN_ARCH_1.0_06062014.pdf

[2] SDN Architecture Overview. Open Networking Foundation. Palo Alto, CA. 2013. Accessed on: December, 2013. [online]. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/SDN-architecture-overview-1.0.pdf

[3] Software-Defined Networking: The New Norm for Networks. Open Networking Foundation. Palo Alto, CA. 2012. Accessed on: April, 2012. [online]. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

[4] Jung, O., Smith, P., Magin, J. and Reuter, L. Anomaly Detection in Smart Grids based on Software Defined Networks. Proceedings of the 8th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS 2019), p.157-164.

[5] SDN MicroSENSE Project. Horizons-EU 2020. 2019.

[6] Gonzalez-Granadillo G., Gonzalez-Zarzosa S. and Faiella M. Towards an Enhanced Security Data Analytic Platform. 15th International Joint Conference on Security and Cryptography (2018).

[7] Github. Discovery-CyberLens Software Tool. Availale: https://github.com/CyberLens/Discovery. Last accessed 2020.