Topic 7 Discussion 2

How does software-defined networking (SDN) help customers with security?

Hello Class,

Software-Defined Networking (SDN) significantly enhances security for customers by providing a flexible and centralized approach to network management. SDN involves the virtualization of network assets, offering greater visibility, scalability, and control. This action moves the network from being made up of individual pieces to a centralized dashboard. A software-defined approach to security functions on the same principle, but instead of virtualizing the entire network, we add virtualized security components. Let’s take a look at the benefits of moving away from a traditional network security approach to a software-defined one(Bocetta, 2022). With the increased network traffic and complex data streaming, SDM, has continued to be in demand by using virtualization for network transparency, through automated security threat detection, security polices application, and access control. SDM, promotes centralized management of sensors, terminals, communication modules, IoT gateways, and other devices.

Network Segmentation: Involves creating subnetworks inside of a larger network, this is called segmentation, which helps compartmentalize and organize your organizations network traffic.

Centralized Remote Management: Virtualized software-based security is managed from a single centralized dashboard. This network security allows an organization to track the security of all employees, and ensure security is consistent for onsite and offsite employees.

Automation: Current firewall architectures do not scale well, and this may interfere with your business’s agility, yet Virtual network firewalls allow you to benefit from the same features as physical firewalls, but they add more agility, flexibility, and scalability(Bocetta, 2022).In addition, Functions that are virtualized, can be updated automatically from licensing to their policies, which a big advantage point of this, makes it easier to keep up with the latest security trends. Last, a virtualized infrastructure will offer a much smoother transition, if you are are planning on migrating a databases.

Scalability: It is far easier to scale virtualized processes and network components due to the fact, they do not require the purchase of new hardware. In addition, due to the security tools that are virtualized, this will allow them to be deployed at will, which allows for seamless growth in operations.

References:

Bocetta, S. (2022, January 16). *Five Benefits of Software-Defined Network Security*. Www.networkcomputing.com. https://www.networkcomputing.com/cloud-networking/five-benefits-of-software-defined-network-security

Wang, T. (2016, July 1). *Benefits and the Security Risk of Software-defined Networking*. Www.isaca.org. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/benefits-and-the-security-risk-of-software-defined-networking