FEATURE

Identifying the security pitfalls in SDN

While a software-defined network can improve application performance and help ease administrative tasks, it can also create new vulnerabilities. Experts offer advice for security teams.

COMPUTERWORLD

Software-defined networks can be a boon to savvy organizations, offering opportunities to cut administrative costs while increasing network agility. But SDN technology can also create security risks, and how you manage those risks can mean the difference between a successful implementation and a disastrous one.

With the SDN architectural model, control of a network is decoupled from the physical infrastructure, which enables administrators to manage network services across different types of equipment from multiple vendors. Organizations can decouple the system that makes decisions about where traffic goes (control plane) from the systems that forward traffic to selected destinations (data plane).

SDN can deliver automated provisioning, network virtualization and network programmability to data center and enterprise networks. The increased network flexibility can help organizations as they move further into areas such as cloud computing, mobile technology and the Internet of Things.

"SDNs are the new architecture for the new age of IT and [off-premises] processing," says Daniel Mikulsky, an IT disaster recovery instructor at the Disaster Recovery Institute International, which provides professional certifications and education programs. "With the rise of cloud services, big data and the consumerization of IT through mobile computing and the Internet of Things, network flexibility and adaptability need to coincide with other innovations in technology."

Demand for the technology is expected to rise: IDC estimates the worldwide SDN market will hit $8 billion by 2018. That forecast includes physical network infrastructure that's already in use, controller and network-virtualization software, SDN network and security services and related applications, and SDN-related professional services.

[Further reading: CoxHealth finds relief in a network overhaul that pushes Layer 3 to the

edge]

And as demand for SDN grows, so too do security fears.

"One of the biggest security issues is that this is still a relatively immature technology, so we don't know for sure what types of exposures are possible," says Frank Cervone, director of IT at the School of Public Health at the University of Illinois at Chicago.

But while there's still much to learn about SDN, security experts who have begun to explore the technology's hidden dangers say there are ways to safeguard your systems.

A technology in layers

While the technology is relatively new, specific vulnerabilities already have been identified within the SDN architecture, particularly the data plane and controller layers.

In the data plane layer, many of the protocols are still new, "so we don't know how robust they really are," Cervone says. "Some of the protocols do not require authentication or encryption, so it's possible that an incorrectly configured component on the network could become an attack vector, inadvertently allowing traffic to be diverted or inspected."

The data plane layer, as with SDNs in general, can also be vulnerable to outages in a natural or man-made disaster. "Given that most major disasters are regional, which will cause physical disruption of network infrastructure, SDNs will need to be configured to meet normal capacity," Mikulsky says.

However, because disaster recovery is becoming increasingly network-dependent, "we can't be sure that the reconfigured network can cope with the additional demands on capacity," he says.

Companies need to ask their network providers if they have contingency plans to add capacity in the event of a disaster. Virtualization is one way to redirect resources, Mikulsky says, but physical capacity needs to be available and accessible.

Also in the data plane, some older data center access technologies are deployed, including tunnels, Virtual Extensible LANs and a variety of bridging protocols, says Chris Krueger, director of cloud and virtualization at Coalfire, a provider of risk management and compliance services.

"Hackers capturing these streams can gain insight into the network implementation, as a result of their payloads being unencrypted and often poorly segmented or secured," Krueger says. "By monitoring and then forging the Data Center Interconnect link traffic, a variety of disruptive and intrusive events may be perpetrated."

Targeting the control plane

Security risks are magnified within the control plane, because "it becomes a single point of failure in an SDN environment and relies heavily on automation," says Stan Mesceda, high-speed encryption product manager at Gemalto, a security technology vendor.

"If the controller is compromised, there are risks of denial of service, misdirected traffic and [exposure of] data at rest or in transit," Mesceda says. "Also, human errors within an SDN controller or orchestration engine can have a ripple effect throughout the network."

SDN controllers will likely prove to be high-value targets -- although, again, it's too soon to know what kinds of attacks companies could suffer, says Brad Hibbert, CTO at network security company BeyondTrust.

"Most vulnerabilities that are leveraged in the wild have patches, but [the patches] have not been deployed due to resource limitations, lack of process and so on," Hibbert says. "When you are talking about network equipment and hypervisors that, if compromised, can have a devastating impact on the risk posture of an organization, these are items that need to be of highest priority and included in your ongoing vulnerability management and patching programs."

Another significant vulnerability continues to be excessive access and lack of administrative oversight on networking equipment and hypervisors, both on-premises and in the cloud.

"As insiders and outsiders -- through a compromised account -- have direct access to manage such network and data center components, they can not only impact availability but also open channels to allow malware and information to slip through and be exfiltrated out of the organization," Hibbert says.

With a typical network, the rule of least privilege is important, adds Chase Cunningham, threat intelligence lead at cloud hosting company Armor. "But with an SDN system, if any one user is granted rights to something they shouldn't have access to, the whole network and literally every asset, item, configuration and database are in danger."

All it takes is a small incorrect configuration and a malicious user. Or an infected machine could access and control or modify items well outside the scope of their intended uses, Cunningham says.

"Malware that can detect if it is on a virtual host and try and 'hop' to the actual control server or entity is also a concern," he says. "That could be an apocalypse scenario, as the malware could theoretically have command and control of everything that is running on the SDN and the entire virtual environment."

[Further reading: Download the full digital spotlight for more on SDN]

One of SDN's benefits is its ability to adaptively respond to a distributed denial-of-service attack, Cervone says. "The software can simply adjust the structure of the network to circumvent the attack rather than just trying to block the attack, which is a significant improvement over past strategies," he says.

But the SDN software stack itself could also be attacked, Cervone says. "If someone were to develop a mechanism that could flood the stack so that it went into overdrive trying to reconfigure the network, thinking that a different type of attack was going on, that could certainly make the network grind to a halt."

Locking down SDN environments

Here's a look at some specific recommendations security experts have for companies planning to deploy SDN technologies.

Be proactive about SDN security. As SDN becomes more common, the attack vectors will likely increase. Organizations need to be prepared for the vulnerabilities and take steps to mitigate them.

You should have a predefined security plan ready when you begin designing a network, Krueger says. Include architectural mandates, and security appliance/device implementation guidelines that have been vetted by your company's chief information security officer and are in keeping with policies and directives.

"Use of SDNs will become widespread in the near future, and by virtue of cloud providers becoming the actual infrastructure for more business-critical workloads, this topic will have greater focus, interest and exposure in the years to come," Krueger says. "Make security a design-in before you build it. Break the cycle of adding security as an afterthought, if that's been the model thus far."

Standard security practices can be implemented to keep SDNs secure, Mikulsky adds. "These entail rigid policy implementation and control, monitoring, scheduled patching and maintenance, as well as the implementation of moving-target defense algorithms," he says.

However, with SDN security, you should adopt exercise and testing scenarios that assume that an attack has been successful. Procedures should include detecting the anomaly, isolating the problem from the rest of the healthy network, and then implementing automated self-healing within the network.

Practice vigilance with network access and user authentication. "The most overt issue with SDN is really careful management of the configuration and ensuring that only those users who need access to certain items or areas of the network are provided that access," Cunningham says.

"Lock down permissions, and double-check regularly that they are configured correctly," he says.

As for authentication, "make sure users are who they say they are but also authenticate applications" and network-function virtualization, Mesceda says. "As new circuits or applications are spun up, make sure that the architecture and applications riding on it are secure and performing as desired."

Maintain the visibility of all of the layers. "The best practices applied to SDN should follow those related to cloud computing and network infrastructure security," says Chris Richter, senior vice president of managed security services at Level 3 Communications, a global communications network operator.

"Level 3's approach to tackling these issues is a multi-tiered, network-based model," Richter says.

Having visibility into the individual layers, how they interact with each other and what systems have access to these layers "is key to detect abnormal activities," he explains. "You cannot defend yourself against something you can't see. Once you can see what is happening, you can determine the appropriate countermeasure."

In addition, it's imperative to have a clear definition of who administers the policy for each layer. "A strong orchestration engine can be designed to balance the business and security needs, but security policies should outline which security functions will be automated," Mesceda says.

Make note of changes as you move to SDN. Cunningham advises establishing a firm and detailed system baseline as the migration to an SDN environment takes place. "Without good knowledge of what is being moved, how can one know what might be changed?" he says.

Keep regular interval images and snapshots of everything, and be prepared to obliterate anything that is acting abnormally. "One bad apple can spoil the bucket with SDN," Cunningham says. "Make sure that even seemingly benign items, such as virtual routers and databases, are only talking to what they need to talk to for operations. There should be no holes or open ports that aren't needed."

Take advantage of threat intelligence

Security threat intelligence can help alert IT managers about new threats to SDN environments. This type of information is available through a large and growing number of sources that are either included with security tools or are available through stand-alone services.

These resources can help you proactively keep up on the latest threats, particularly those most likely to hit your company or industry.

"We use our expansive view of the threat landscape to set a baseline for normal traffic," Richter says. "The nascent but quickly developing area of threat intelligence is key to navigating the escalating cyber landscape we face."

Keep your network security program up to date. Security is not static, and with SDN there will be ongoing changes in threats and vulnerabilities, and in the tools used to keep systems secure.

You should upgrade your defenses as new products become available, and update your policies to reflect new realities.

"Security is an ongoing business; do not set it and forget it," Mesceda says. Unfortunately, not everyone heeds that advice. "Often, critical patches are not deployed, systems are not re-evaluated often enough. And the architecture can quickly become vulnerable without a dedicated approach to security," he says. "Many companies use a phased rollout approach, but they fail to revisit earlier rollouts to ensure the system still adheres to security best practices."

Bob Violino — *Contributing writer*

Bob Violino is a freelance writer based in New York.

The whiteboards of tomorrow: 3 interactive displays

View 1 Comment