Virtualization as Vaccine?

Heartbleed is only the latest security bug to hit the news. Can SDN help inoculate the networks of the future?

By Julie Knudson | Posted Apr 21, 2014

2

As enterprises rush to plug the holes created by the Heartbleed bug, administrators are looking for new ways to protect against threats. Software defined networking (SDN) may offer solutions. It has some real advantages, but can't do everything. Know its strengths to decide whether it can help keep your network secure.

Security Advantages of SDN

Related Articles

- Visibility Challenges and Solutions in Virtual Environments
- How IT Pros Can Take Control of Their Virtual World

Looking at the threat landscape, some scenarios fall neatly into SDN's wheelhouse. Dan Pitt, executive director at the Open Networking Foundation, said it's very good at identifying when something just doesn't look right, such as "anomalies in traffic patterns that suggest something is amiss." When these suspicious activities are spotted, SDN gives administrators the ability to react quickly in a couple of ways. One is to immediately modify how network traffic is handled. Administrators can change its direction, isolate it, or force it through an analysis program.

Another key advantage is the very nature of a software defined environment. "If some new type of threat were to appear, somebody could write software to figure out how to handle that and deploy it very quickly," Pitt said. "You don't have to wait for vendors to go home and update their proprietary operating systems and software." SDN therefore addresses one of the issues enterprises encounter with vulnerabilities like Heartbleed, where components from servers to firewalls may harbor the bug and where administrators could be relying on multiple vendors to provide patches.

An example of a specific exploit that fits right into the SDN model is a distributed denial of service (DDoS) attack. "DDoS attacks are actually good ones to detect in the network, and SDN is a very useful tool for that," said Curt Beckmann, principal architect at Brocade and co-chair of the Forward Abstraction Working Group (FAWG) at the Open Networking Foundation. When suspicious behavior such as a DDoS attack is detected, administrators can then "alter the behavior in the network to deal with the nature of the attack you're experiencing without impeding other kinds of activities on the network."

Threats that SDN Can't Address

Of course, some security threats don't lend themselves to an SDN-based resolution. Data exfiltration is one example. "When something actually gets into a compute environment and starts harvesting stuff from inside, that's well beyond the realm of SDN," Pitt said.

Where an exploit targets a largely self-contained system, like a desktop, "SDN really isn't suited for that," said Eric Johnson, CEO of ADARA Networks. It may offer some limited capabilities to relegate the vulnerability to that particular system, but an SDN environment is "not positioned to help" with an exploit of that nature. When traffic moves along the network, SDN shines. But when that activity is held within a single system or component, SDN can't monitor and manage what's going on.

Making the Most of SDN for Security

Enterprises can take steps to maximize SDN's security perks. Administrators should prepare to leverage the ability to very quickly move services from one component to another, said Karthikeyan Subramaniam, chief architect at ADARA Networks. Hardware, operating systems, hypervisors, application servers, databases—they all serve their purpose within the infrastructure. "From the administrator's perspective, they have to understand their components," Subramaniam explained. "They always need to line up the alternatives." Any one of those components could be vulnerable. In fact, several of them could be vulnerable at the same time. That's where reaction time comes in. "If there is a zero-day vulnerability, use SDN to send the services off the vulnerable component out to different components," Subramaniam said. This quick action will allow the enterprise to continue providing services even while the original components are out of the loop being patched.

Another opportunity exists even in more hardware-based infrastructures where various tiers touch, such as the connection points between a database of available products and the web interface customers use to choose which product they want to buy. "There are tiers of server functionality or workloads, and they're isolated through routers," Beckmann explained. Historically, physical, hardware-based routers were the preferred method of linking those tiers, but now software routers are stepping in with some specific capabilities. "The soft routers are essentially where you insert your protection or where you add detection capabilities," Beckmann said.

This strategy can be particularly useful in enterprises where the various tiers—web, business logic, databases, etc.—have been developed by different teams. "Whether it's malicious or not, it's certainly easy to have a bug in one version of code and you don't want somebody in the web tier to go and corrupt your database," Beckmann explained. Through the isolation of things through these virtual routers, enterprises have the tools they need to "live in the dynamic world of DevOps, where you're constantly adding new features and new capabilities and extending things to new spaces and yet provide an acceptable level of protection," Beckmann said.

To enable the collaboration and connections that power business activities, today's network environments are, by their nature, open. But SDN may provide administrators with the right tools to maintain security even in that sort of interconnected network. "What they need to think about is installing something that provides an overlay to harden what, by itself, is a porous environment," Johnson said.

Many parts of the network have been developed in silos, which contributes to the problem. Johnson said it often creates gaps in security because developers don't always consider what happens when packets are handed to another part of the system. "If they put SDN in and it's commercial-quality, they can solve a lot of the porous types of exploits that exist in all these systems."

As enterprises continue to increase the amount of virtualization within their networks, Pitt said one key to maintaining a good security posture is to avoid complex infrastructures. "I would urge them to simplify the network infrastructure as much as possible. Then the control becomes separate and much more readily amenable to dynamic modification based on decisions or conditions that could have to do with security or something else." This allows administrators to change the network's behavior at a moment's notice from a centralized place. "You're then in much better shape to guard against and react to threats," Pitt said.

Photo courtesy of Shutterstock.

Julie Knudson is a freelance writer whose articles have appeared in technology magazines including BizTech, Processor, and For The Record. She has covered technology issues for publications in other industries, from foodservice to insurance, and she also writes a recurring column in Integrated Systems Contractor magazine.

0 Comments **(click to add your comment)**

Comment and Contribute

Your name/nickname

Your email

Subject (Optional)

Comments

(Maximum characters: 1200). You have 1200 characters left.

Type the text

Privacy & Terms

reCAPTCHA™ stop spam. read books.

Submit