Five Steps to Protecting your IT Infrastructure

vmware

Five Steps to Protecting your IT Infrastructure

Over the past decade, federal agencies have taken full advantage of technology advances to provide more and better services and capabilities to employees and constituents. Today, agencies routinely offer teleworking arrangements to employees, allow users to collaborate with other decision-makers without leaving the office, enable employees to work on the fly via mobile technology, incorporate social media into communication to citizens, and offer a host of online-based services to the public.

Contents

While these advances enhance productivity and citizen satisfaction, they also introduce many more points of potential network vulnerability. At the same time, hackers have gotten much more creative and hacking techniques more sophisticated. Add that to a mountain of digital data that can prove irresistible to cybercriminals, and it becomes a never-ending fight to keep cybersecurity under control.

The sheer number of cyberattacks today continues to increase at a staggering rate. The Government Accountability Office (GAO) reports that the number of information security incidents reported by federal agencies increased by more than 1,000 percent between 2006 and 2014. Perhaps even more alarming, about one-third of cyberattacks aren't detected by civilian agencies, according to a 2013 report by the OMB. And it's expensive; a May, 2015 report from Ponemon Institute found that on average, the cost of a data breach is about $154 per record, which can add up to millions per data breach.

The sheer number of cyberattacks today continues to increase at a staggering rate. The Government Accountability Office (GAO) reports that the number of information security incidents reported by federal agencies increased by more than 1,000 percent between 2006 and 2014.

At the same time, the threat landscape is a moving target; threats continually change, and hackers continually come up with new techniques. The federal government is aware of these changing threats, and there are many mandates and regulations agencies must comply with to ensure that IT infrastructure is protected such as COBIT, NIST800-53, ISO/IEC 27001, ISO/IEC 15408 and ITIL. They demand that government agencies secure and protect the confidentiality, integrity, and availability of information systems and the data processed, stored, or transmitted by them.

All of this, taken together, often means that agencies' existing IT infrastructures—many the result of a patchwork of legacy equipment and applications, manual processes, varying degrees of integration and inadequate visibility—can't adequately protect an agency's network and data. The IT infrastructure that will fully protect an agency's network and data today is one that follows the principal of Zero Trust, which assumes that no network traffic can be trusted. That type of architectural shift is only possible with a combination of virtualization, automation and micro-segmentation.

Five Steps to Protecting the IT Infrastructure

1. Make sure your basics are in place and up to date

Making sure the "bones" of your IT infrastructure are updated and secure can go a long way toward mitigating problems. That means periodically evaluating and upgrading your mobile device policy and infrastructure, cloud solutions and disaster recovery/business continuity strategy. Do the same for any on-premise networking and compute equipment in data centers.

There are other important protections that should be table stakes for every IT infrastructure today. These focus on protecting the network perimeter, operating systems and servers, the host, and data itself. The tools used for protection can vary, and include not only firewalls virus scanning software, but identity and access management, a Virtual Private Network (VPN), intrusion detection, packet filtering router, host-based intrusion prevention and Data Loss Prevention (DLP) tools. Finally, every IT infrastructure today should use some type of big data analytics, which allows information security specialists to analyze large, disparate

data sets to find patterns and draw conclusions on where and when cyberattacks are likely to occur.

Remember, though—these are just the basics. These tools, while extremely important, are not robust or complete enough to ensure full protection from cyberattacks. The breadth and depth of threats today requires a more potent approach.

2. Establish effective security policies

In many organizations, policies often get short shrift, but when it comes to information security, they are the underpinnings of a successful strategy. Without a good security policy, critical procedures can easily be ignored.

While all agencies today have policies related to cyber security, there is little standardization about what is included, and varying degrees of enforcement. In the past year, however, federal leaders have issued a host of guidance on crafting effective security policies—guidance agencies can use to improve their security policies.

NIST's Framework for Improving Critical Infrastructure Security is an indispensable guide for helping agencies create policies around identifying, protecting and defending their assets. It also includes guidance on how to develop an incident response plan, restore capabilities or services that were compromised during a cybersecurity event, and develop a common language for internal and external communication of cybersecurity issues.

NIST's Framework for Improving Critical Infrastructure Security is an indispensable guide for helping agencies create policies around identifying, protecting and defending their assets.

The current administration also has continued to push the cybersecurity envelope. Earlier this year, U.S. CIO Tony Scott launched a 30 day "Cybersecurity Sprint" to rapidly improve agencies' cybersecurity, and the administration plans to use lessons from that exercise to develop more specific guidelines for civilian agencies.

While the specific policies for agencies may not be identical, all comprehensive security policies should include these elements:

- Define roles and responsibilities of employees handling sensitive information
- Periodic security awareness training for employees
- Explaining the cybersecurity chain of command
- Acceptable use and password rules
- Mobile device rules
- A methodology for continually revising and updating documents to reflect current technology, legislation, business objectives and threats
- Identifying and working with sensitive information

3. Virtualize whenever possible

Virtualization today is a mature discipline; nothing is off limits. That means that in most cases, the decision about whether to virtualize comes down to cost. But more than 90 percent of the time, the benefits of virtualization far outweigh the costs. There are many benefits to virtualization other than cost savings, though—it is an efficient path to cloud computing, frees up the time of IT staff, and reduces power, cooling and square footage requirements.

Virtualization also improves security. By virtue of turning physical hardware containers into software containers, for example, it's easier to build automation into that layer, and automation is a basic underpinning of better security. On the network side, because virtual networks are isolated from other virtual networks and the underlying physical network,

they can protect the underlying physical infrastructure from attacks initiated by workloads in any virtual network. Network virtualization also enforces segmentation between network segments or tiers. That means communication within a virtual network never leaves the virtual environment.

The automated nature of virtualization also provides a rich set of data that allows security specialists to make better security-related decisions. For example, it is easy to see what kind of software is running inside the system, who is logged into it, the level of sensitivity of the data, and how that system is attempting to communicate with another system or the outside world. By analyzing all of that data, the resulting security decision will be much more effective and accurate.

4. Move away from a perimeter-only defense

Traditionally, organizations have focused the bulk of their security budget and resources on protecting the network perimeter with firewalls, intrusion detection systems and two-factor authentication for external users. While those methods are always a good basic defense, they simply aren't good enough, given the reality of today's threat landscape, to fully protect the IT infrastructure. That's because it is based on two faulty assumptions—that you can trust everybody who enters the network, and that perimeter-based tools can succeed 100 percent of the time.

That means that some of the time, unauthorized people can break through and once they do, they have full access to whatever data and other resources they want. Research from SafeNet backs this up; it found that 44 percent of IT decision-makers say their organization's firewall has been breached or don't know if it has been breached, and that more than 60 percent were not confident that data would be secure if unauthorized users were able to get into the network.

The solution is moving to a security model that assumes that nobody can be trusted and that every device or person who communicates within the network must be visible and tracked. It also requires that everything within the network is just as protected as the network perimeter itself. It's such a hot-button issue that Gartner ranked moving away from perimeter-based security as one of the top ten strategic technology trends of 2015.

5. Transition to a software-defined data center

The idea behind the software-defined data center is simple: By virtualizing all compute, networking and storage in the data center and automating all provisioning and management in a software layer, resources become more automated, flexible, cost-efficient, easily managed and secure.

Because everything in the SDDC is software-based, it's easy to insert protection into the storage, network and compute layers without anybody even knowing it's there. In the compute layer, for example, the IT team can insert authorization policies that allow the compute power only to run in specific environment and only with specific software.

The SDDC also makes it much easier to quickly provision and decommission resources. That means it is simple to stand up services when needed and destroy them when finished. The less time services are in play, the less they are a potential target.

The SDDC also makes it much easier to quickly provision and decommission resources. That means it is simple to stand up services when needed and destroy them when finished. The less time services are in play, the less they are a potential target.

Moving to a software-defined data center also allows agencies to enforce a Zero Trust architecture—one of the most important steps in securing the IT infrastructure today. In this model, security travels with the data, both inside and outside the network. The software-defined data center achieves this by segmenting network traffic at a very granular level. It compartmentalizes both east-west traffic—the lateral traffic that occurs inside the network—and north-south traffic, such as a hacker trying to access the network. This method, called micro-segmentation, is the best way to permanently harden the IT infrastructure against security breaches and stop the patchwork approach to security.

Meeting the Challenge

Making the necessary changes in IT architecture to strategically tackle cybersecurity means enhancing automation, implementing micro-segmentation and enforcing Zero Trust. One implementation strategy that helps agencies achieve these goals without undue expense or forklift upgrades is VMware's NSX, which provides the networking and security foundation for IT infrastructure. Ideal for software-defined data centers, NSX enables security managers to segment network traffic down to the micro-segmentation level.

NSX does this by turning each segment into a virtual segment. Security managers can then create as many virtual segments as needed, as quickly as needed, and program them to be provisioned automatically and on demand. Once the firewall policies are set, the system takes over and intelligently applies the correct rules to the correct firewalls. Those policies follow workloads as they move through the data center. In addition, NSX allows security managers to set different policies for different virtual networks.

NSX also fully supports the Zero Trust model by using micro-segmentation to wrap controls around small groups of resources, down to individual virtual machines. Enforcing Zero Trust in a standard infrastructure model would mean buying, configuring and managing a separate firewall for every server, desktop or virtual machine connected to the network. With NSX, each device or virtual device can be compartmentalized in its own separate firewall, and the IT infrastructure can work from one centralized rule set.

Finally, NSX makes all types of mobility much more secure. Unlike typical models, which tie security to the device, NSX ties security to the user. By moving from a device-centric to user-centric security model, it no longer matters what device a person is using—a smartphone, tablet or virtual desktop—the same security principles apply. NSX bases the security rules it applies to the person accessing the device.

By employing the three principles that make IT infrastructures much more secure—automation, the Zero Trust model and segmentation—agencies will be well positioned to protect systems, data and people not only in the near term, but in the future. ■

Making the necessary changes in IT architecture to strategically tackle cybersecurity means enhancing automation, implementing micro-segmentation and enforcing Zero Trust.

About Activate

activate

Activate combines deep buyer insights with a content-led nurturing methodology to engage prospects and convert them to customers.