Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 12, Issue 5

Cybersecurity Goes Mainstream

By Rob Marson

Back to the Future

I recently read an article online entitled: "Virtualization is Going Mainstream". The dateline was January 1, 2006. It's a good reminder that while the service provider industry working on deploying virtualized networks, the concepts and technologies themselves are not new.

Cybersecurity, specifically securing access to physical and virtual networks and resources, is another key area. A recently released study by Kasperksky Labs concludes that when a security incident involves virtual machines, the recovery costs double compared to that of a traditional environment. It is clear that some of the operational challenges encountered from the enterprise IT experience could be harbingers to some of what awaits service providers as they race to virtualize their networks and implement new technologies such as Software Defined Networks (SDN) and Network Function Virtualization (NFV).

The Days of Security-Through-Obscurity Have Ended

Service provider networks are complex by nature – they span multiple technologies, vendors, geographies, and support millions of end users. Services will extend across wired and mobile networks, and span virtual and physical infrastructure. Equally complex are the business processes and operational challenges to order, administer, maintain and scale services. Management, security, and visibility strategies must also become flexible and adaptable enough to address hybrid environments that encompass both legacy and newly virtualized functions. It's vital to remember that services traverse heterogeneous, physical and virtual networks.

Service provider networks have, in the past, been shielded from a lot of security threats because of obscurity. Proprietary protocols and custom hardware required specialized skill sets. That all changes with SDN and NFV. Admittedly, there are many considerable and important differences between enterprise virtual machine (VM) workloads and the data plane intensive virtual network functions (VNFs) that will be used by communication service providers like components of a mobile evolved packet core (EPC) such MMEs, SGWs, and IMS core elements. Therefore, implementing mission-sensitive networking applications using cloud technologies may impact performance in unforeseen or unacceptable ways, require accurate system configurations, and could introduce new unintended security risks.

Traditional hardware-based networks are not immune from security attacks either. In the past, attackers were primarily targeting infrastructure devices to create denial of service (DoS) situations. Increasingly, networking devices such as routers are becoming a high-value target for attackers. By penetrating network infrastructure attackers can gain access data flows as well as launch attacks against other parts of the infrastructure.

Take, for example, the recently SYNful Knock attack. While the attack could be possible on any router, the targets were Cisco routers and involved a modification of the router's firmware image creating backdoors for attackers. The backdoor password provides access to the router through the console and Telnet. This attack isn't the result of a problem or vulnerability the router itself the result of attackers

obtaining administrative credentials allowing them to load a modified version of operating system software. The keys to this attack are nearly always privileged user credentials.

The Hypervisor – Protect at all Costs

There are many potential security issues with the various components of a virtualized infrastructure, and no component is more critical than the hypervisor – the foundational element of virtualization. The hypervisor is a piece of software that provides abstraction of all physical resources such as CPU, memory, network and storage. It enables multiple computing stacks consisting of an operating systems, middleware and applications to be run on a single physical host. Individual computing stacks are encapsulated into instances called Virtual Machines (VMs), which are independent executable entities. VMs are also referred to as "Guests" and the operating system (OS) running inside each of them as "Guest OS".

The hypervisor performs many of the roles a conventional OS does on a non-virtualized host or server. It provides isolation between the various applications, or processes, running on a server. The hypervisor controls VM access to physical hardware resources as well as provides isolation among VMs. There a number of security threats to the hypervisor and many of these threats emanate from insiders, such as virtualization, network, cloud and security administrators, in addition to threats from external attackers. The National Institute of Standards and Technology (NIST) recently published some important research in a Special Publication 800-125-A on the potential security threats to hypervisors, and recommendations to mitigate them.

Don't Forget to Lock the Side Door

Rogue VMs pose significant threats to hypervisor security. Rogue VMs can initiate side channel-attacks from target VMs running on the same physical host. A rogue VM could hijack control of the hypervisor, performing malicious actions such as installing rootkits as well as launch attacks on another VM on the same virtualized host. A rogue VM could also manipulate virtual switch configurations and compromise isolation between VMs to snoop on east-west network traffic between VMs. More often than not, attacks launched from rogue VMs are permitted because of incorrectly configured settings and parameters.

The Communications Fraud Control Association (CFCA) estimates that Telecom Fraud costs the industry over $40B USD annually.

Other attacks on the hypervisor include resource starvation leading to denial of service attacks, or a hypervisor providing privileged access to a virtual security tool that could in turn be exploited. A misconfigured VM may consume shared compute and memory, resulting in other VMs being starved. Hypervisors provide privileged interfaces which can be targeted by rogue VMs. Privileged operations such as memory management can be invoked by rogue VMs and executed by the hypervisor.

Identity is the new Perimeter, Especially for Privileged Users

Traditional approaches to privileged identity management emphasize perimeter-based security controls. Relying solely on firewalls and perimeter-based security strategies still expose networks to insider threats, a growing risk. Increasingly, external hackers are targeting privileged users with sophisticated phishing attacks. Cyber-attackers commonly use a combination of social engineering and malware, often in the form of an email phishing attack. Specifically, they target an organization using information harvested via social engineering, social media, and open source data, and then lure unsuspecting users into downloading malware onto their computers. The attackers' objective is gaining account credentials or personally identifiable information, contact information and links to other accounts, including those to networks. Attackers typically remain present for long periods of time, moving laterally across systems and organizations. Incident response firm Mandiant has reported that the average mean time to detection for network security breaches is 205 days. During this phase, it's likely that the attacker

is using the legitimate credentials. As a result, service provider network and security operations teams are increasingly the target of phishing attacks. In a recent case, a service provider's network was compromised in this fashion allowing hackers access to modify the configuration network firewalls in order to create persistent pinholes into the network for snooping.

Fraud is another critical threat facing communication service providers. The Communications Fraud Control Association (CFCA) estimates that Telecom Fraud costs the industry over $40B USD annually. This equates to almost 2% of revenues. The most common types of fraud include but are not limited to subscription identity theft and International Revenue Share Fraud (IRSF). This occurs when hackers obtain Subscriber Identity Management numbers (SIMs) from service providers and use them for international roaming status to begin placing outgoing international calls in order to exploit some countries' high termination rates, or inflate traffic into other high value numbers with the intention of sharing any revenues generated. PBX (Private Branch Exchange) hacking is one of the leading types of fraud globally. In this scenario, a company's PBX system is compromised and long distance/international calling access is provided to third parties. The CFCA estimates that this type of fraud costs close to $5B annually in lost revenue. Often PBX administrator credentials are used to change call routing configurations. New hosted and virtual PBX services create new types of attack vectors. Often, these types of fraudulent activities are in collaboration with internal employees and collaborators.

Passwords are the Keys to the Kingdom

Privileged identity access management (IAM) is a key challenge for service providers. On average, a typical user has on average 35% more access rights than needed. In another example, a service provider had roughly 4,000 employees, but over 40,000 privileged user accounts. The boundaries of networks, and between elements within the network themselves are becoming more blurred. Service providers will distribute virtualized infrastructure and VNFs throughout their networks. New configurations, new devices, and new virtualized functions can appear and move. The degrees of automation possible with technologies like SDN and NFV, along with the emergence of the Internet of Things (IoT), requires a redefinition of the term "identity". New business models enabled by these technologies further opens up service provider networks to a growing community of third-party users. Furthermore, users are accessing network resources from a variety of devices, both fixed and mobile, and from any variety of locations. Traditional, human-focused IAM systems must now accommodate people, processes, and systems.

BT along with industry research firm Gartner estimate that 65% of cyberattacks exploit systems with vulnerabilities introduced by configuration errors.

Finding backdoors within networks can be challenging. Finding modifications to network configuration settings that create security pinholes is even more daunting. This challenge is compounded by new technologies such as SDN and NFV which bring more dynamic, programmatic network environments. Incorporating proactive network configuration discovery and auditing is more important than ever, both from a security standpoint as well as from a performance management perspective.

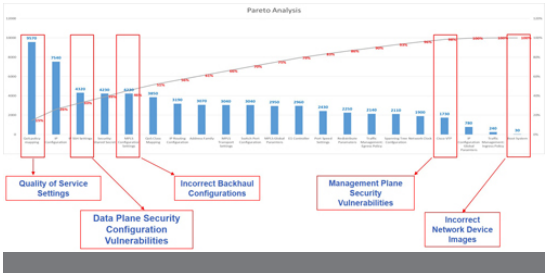
Check, Re-Check, Check Again and then Check Some More

VMs are typically created from templates which specify key configuration criteria including processor and memory load. In order to assure correct implementation, VMs require a "Gold Image" which defines the set of configuration parameters such as information about the Guest OS, version and patch level. It is important to proactively scan active VMs to ensure that they are properly configured when compared to the "Gold Image". NIST explicitly recommends that the VM configuration be checked for compliance to configuration settings in these Gold Images in order to minimize configuration errors that may increase the security risk. This is distinctly different from the monitoring of inter-VM traffic. VM "Gold Image" must also be protected with strict access controls. Cloud architectures result in an elastic perimeter. More users throughout an organization, as well as trusted partners increasing risk of data leakage. Privileged user identity and account management strategies to both the hypervisor, consoles and data bases is essential.

Service providers spend considerable time and money isolating the source of network performance issues. Processes often include deploying test equipment, capturing traffic, analyzing data, only to isolate the cause of an issue to be the result of a setting on an individual router or switch. Service providers confirm that up to 60% of their network outages and degradations

are caused by network configuration errors. This is only going to intensify with NFV which will bring with it orders of magnitude more configurable parameters along with more interdependencies. Ensuring that servers, the VNFs themselves, and all supporting systems are correctly configured, and stay correctly configured, is will be to assure service delivery performance and service level agreements.

Analysis of backhaul network configuration for a mobile service provider spanning more than 10,000 different network elements or functions from multiple suppliers and close to 30 million configurable parameters identified a considerable number of configuration errors impacting subscriber experience. Numerous security vulnerabilities were also detected.



Configuration errors enable 65% of cyberattacks and cause 62% of infrastructure downtime according to a recent published research. UK headquartered service provider BT along with industry research firm Gartner estimate that 65% of cyberattacks exploit systems with vulnerabilities introduced by configuration errors. A review of Annual Incident Reports published by the European Union reveals that 25% of reported incidents in 2013 were the result of human error or malicious actions. The report goes on to cite that incidents caused by malicious actions, had long recovery times (53 hours) on average resulting in 11,600 user hours lost. Moreover, most operators do not correlate the relationship between malicious attacks and outages. The all-IP nature of modern mobile networks creates an expanded attack surface to exploit security vulnerabilities.

The definition of identity access management must expand to include people, processes, and systems and provide contextual awareness.

Discovering and analyzing network configuration parameters along the service path is key to be able to isolate where exactly customer impacts are occurring, and where hidden security vulnerabilities may lurk. Similar to gold standard VM image management in a traditional IT environment, service providers require strategies to import, update, define and manage the lifecycles of “Gold Standard” service templates. Furthermore, using these templates in a proactive, automated fashion to scan the configuration of service chains helps eliminate configuration issues in the first place.

Identity and Configuration – The Keys to Improved Network Cybersecurity

The recent increase in sophisticated, targeted security threats by both insiders and external attackers has increased the awareness and urgency for comprehensive security strategies. Achieving “network security through obscurity” is no longer an option for service providers.

Privileged identity access management strategies must provide granular access control, flexibility, auditability and ease-of-use. Identity data provides critical forensic information. Correlating security events with network configuration data changes or anomalies provides a powerful strategy for service providers to prevent, detect, neutralize and threats. Behavioral analytics helps service providers predict.

Network configuration management is a process by which configuration changes are proposed, reviewed,

approved, implemented, verified, and re-verified. Implementing configuration management best practice is not only essential to assure network quality but also to mitigate security risks. Often vulnerabilities are the result of misconfigured network security policies.

The definition of identity access management must expand to include people, processes, and systems and provide contextual awareness. Technologies including SDN and NFV drive the need for new approaches to holistic network security. The notion of a Secure Network Auditing Platform has emerged which combines identity access management, continuous network configuration data auditing, with value-added network behavior analytics. Learning expected network behavior, correlating network security access events with network configuration changes allows service providers to detect anomalies in order to anticipate, prevent, pin-point, and isolate security policy violations.