Mark Wollerman

4/6/2015

Enterprise Info Securtiy

Instructor Dr. Phil Lunsford

Instructor Mrs. Constance Boahn

Securing The Enterprise Network – Best Practices

Mark Wollerman

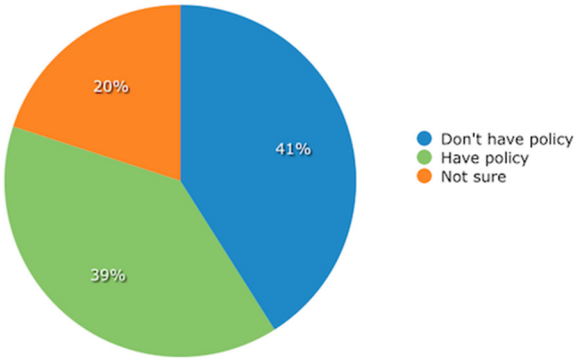
East Carolina University

Abstract

The following research topic looks at different approaches to securing the enterprise network. In this topic we will discuss the best practices that can bring additional security to the enterprise network. In today's network enterprise attacks can be more sophisticated that what the modern security engineer can expect. The modern enterprise network has changed allot since the late 90's and early 2000's. Today's biggest concerns include, user brought devices, Virtualization, Account Schema's, Emails and Network security.

Today's enterprise network is facing a new challenge called Bring Your Own Device or BYOD. BYOD can be considered cell phones laptops computers or other devices that connect to the enterprise network. BYOD brings new aspect to security issues on an unprecedented scale. Devices outside the network bring threats in that are

unprotected at the source. The modern enterprise network connects devices that are attached to the network a typical enterprise network will then push correct updates to these machines anywhere from vendor patches to antivirus. BYOD on the network can bring in these unattended exploits to the network. The biggest of these exploits being Zero Day attacks on mobile devices. According to Lyon, C., & Osterman, M. (2014). "Zero-day vulnerabilities are software vulnerabilities that are actively being exploited the same day of (or prior to) their discovery. In this scenario, antivirus vendors do not have enough lead time to identify and ship updated signatures before users are at risk". These unattended updates and security concerns for mobile devices leads to giant gaps that hackers can exploit. According to Humphries (2014) "Only 49 percent of respondents implement security updates when they're released." From a enterprise network of 5000 employees that means 2,500 BYOD devices are walking security concerns. Another big concern with BYOD is that most organizations do not have a BYOD policy in place. It is estimated that 39% of organizations do not even have a policy in place for BYOD. While these facts may not directly effect the network they can pose serious threat. The biggest threat to BYOD is idea it creates a window for hackers to see everything including company data without anyone even knowing about it. According to According to Humphries, D. (2014, August 1). "it is estimated that of all BYOD devices Over half of respondents have transferred company files to their own devices.". This estimate means



that critical enterprise data is literally sitting on devices and most importantly emails and other sensitive data connected to peoples smart phones that are available for the world to see. The perfect solution would of course be to block all usage of BYOD. Combatting the BOYD issues requires multiple steps the first being to draft foundation policy's that address what is allowed and what is not allowed. Security concerns show that could information will still be available in the cloud and accessible by multiple means however restriction by devices could be controlled with file encryption.

In a perfect IT environment virtualization is would be on every machine. Machines clustered together saves money by sharing hardware resources. Instead of the enterprise environment needing to pay for 2000 machines with upgrades and cost of service and equipment that goes with the machines such as power strips keyboard mice and monitors A simple VM ware machine can host thousands of computers and reuse existing machines in place for years beyond the life of the machine. Organizations can also use thin clients to remote access into the VM server. From an IT perspective virtualization has many advantages. With VM ware technology a machine can be created restarted and reset all done remotely at the click. The idea of virtualization containing all machines within a single shell is every IT administrators dream however like all other systems they are subject to flaws. According to Fogarty, K. (2013, May 13). "It's theoretically possible for hackers to attack the hypervisor layer specifically, or to take over a VM and use it to attack other VMs, ". With an enterprise environment this can spell disaster. A simple VM machine with thousands of users can become easily a giant army of zombies. Additionally Machines that are simple images of the original machine can be re-implemented but what happens when those images become out of

date? According to Fogarty, K. (2013, May 13). “"You can take a snapshot of a virtual machine and write it off to disk so you don't have to recreate it the next time, or for disaster recovery. Just fire off one of these virtual machines sitting in offline libraries. But for the most part they're not being kept up to date with A/V signatures and patches”. Not keeping up with patches from old images can present huge problems especially if those patches are no longer valid because of a vendor change such as new antivirus or a new updates from Microsoft. Keeping an up-to-date baseline image is critical as this can save time and money assuming the VM machine suddenly goes offline. Another big concern with Virtualization in the enterprise networks is known as Sprawl. According to VMware (2012) “Virtual machine sprawl is one of the biggest concerns facing many companies using desktop or server virtualization. The ability to quickly create virtual machines without the disciplines and controls of the physical world results in machines being provisioned unnecessarily”. Not only does sprawl present a problem for the existing network but also unused desktops that are powered on and left open instead of logging out. Sprawl presents security concerns since these desktops and servers are on the same network with other resources can allow hackers to do a great deal of damage. Spawl also costs money to the large scale organization. According to VMware (2012) “A typical company with 1,000 virtual machines—with five percent of machines created without proper business justification and another five percent over-provisioned—could easily save over USD $100,000 to USD $150,000 in capital expenditures through better control of the front-end provisioning process”. To combat sprawl a system administrator should have in process a good cloud automation platform software. Cloud automation can help according to VMware (2012) “A cloud automation platform should provide

exception reports that help identify stranded, inactive, and abandoned machines and automate the workflow associated with reclaiming those resources." Software like this can simply look at the resources being used and determine if there is activity.

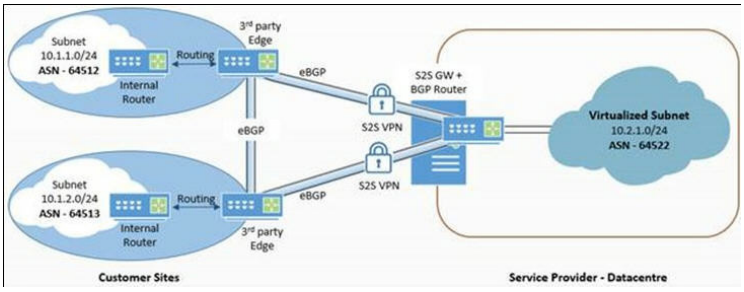
Securing the enterprise network also happens at the rudimentary level. Creating an solid Active Directory forest for the domain is key however from a security standpoint the nuance of the Active Directory ties into exchange closely in an enterprise network the user name can be the most critical way to establish how users are set up. A good scheme to remember is that the more protection to the network the better. For example suppose I create a new user Joe Smith in a typical smaller environment the username would be jsmith@contoso.com . However what happens when there are two Joe Smith's or three Joe Smith's ? A typical route to follow and by default in Microsoft Exchange is to create a numbered alias such as jsmith1@contoso.com and jsmith2@contoso.com this additional number adds security to the network and allows users not to be identified so quickly. Suppose an outside hacker wants to gain access to critical files in the network. A simple google search is all it takes, for example a hacker could type in who is the president of Contoso corporation or who is the director of finance? Of course Wikipedia responds with Doug Niedermeyer without any effort the hacker can assume the username for Doug Niedermeyer is dniedermeyer@contoso.com or dniedermeyer1@contoso.com or dougniedermeyer@contoso.com since this is a unique last name they would probably be correct. A better approach to this situation would be to create a schema when setting up the AD forest and usernames to encode user names from the beginning. For example instead of jsmith@contoso.com creating all usernames with last name first

initial and random number smithj192@contoso.com this makes it more difficult for hackers and spammers alike to send malicious emails to Joe Smith and also makes it more difficult to gain access to Joe's account. As best practice changing Active Directory usernames to this schema can provide additional security to the network.

Email is one of an organizations biggest weaknesses. A typical security administrator will constantly worry about spam, phishing emails and infected attachments. Email is one of the biggest single points of failures in a network a malicious email with corrupt and infected attachments will still come across the network. One of the biggest concern facing the enterprise network is called a Directory Harvest Attack. According to Roust,M. (2005) "A directory harvest attack (DHA) is an attempt to determine the valid e-mail addresses associated with an e-mail server so that they can be added to a spam database." In the enterprise network this type of attack can progress over the course of months or years the attack unlike a DDOS attack and simply build a database overtime and remain undetected. According to Roust,M.(2005)" involves sending a message to the most likely usernames - for example, for all possible combinations of first initials followed by common surnames. In either case, the e-mail server generally returns a "Not found" reply message for all messages sent to a nonexistent address". An email system is typically set up with an exchange or Linux server behind a firewall or DMZ. This is typical in smaller organizations however what about the enterprise network. In order to combat DDOS attacks and floods of email a third party edge hosting device should be used instead. A spam filter at the edge of the network allows incoming mail flow to reach the third party first. This service takes the email inspects it and forwards it on to the correct exchange

server or holds it if it looks like spam. The key difference is that the exchange server will never have direct access to the outside network and the edge device will not send a "cannot find user" back to the sender. This allows risk transference in the event of a spam attack and also helps keep information about the email setup secure. A typical system like this is also user driven, for example when the edge device does receive the email and it looks like spam the user will receive a notification that they may have spam. The user can then login to the edge device, inspect the email on the device at the edge instead of the local machine minimizing risk to the user. Once the user opens the email they determine if the email is safe to release it or not the smart function built into the edge device can determine if this email is ok to release next time.

Keeping the network safe on the enterprise level requires the enterprise network to be one step ahead of hackers. From the basic network security administrators are taught to implement a control strategy that includes a router with ACL's and permissions, a DMZ for creating security and various other security functions such as software and hardware security controls at the LAN. The enterprise network needs to be one step ahead by implementing a transfer of risk from the core network to a third party service. This strategy can be implemented by utilizing 3rd party gateway with BGP at the enterprise site edge. This implementation greatly reduces the risk of an attack of a gateway router that sits directly on the edge of the LAN. Creating edge redundancy not only takes the burden of attack off the core network but also builds in redundancy be being able to route to different edge devices.



According to Microsoft (2014) “If the BGP router at Enterprise Site 1 cannot connect with the CSP datacenter BGP router because connectivity has failed, the Site 1 BGP router dynamically begins to learn the routes to the CSP network by using the other Enterprise site (Site 2), and the traffic is seamlessly rerouted from Site 1 to Site 2 to the CSP.” If gateway 1 on the edge goes down due to a DDOS attack gateway 2 can dynamically route traffic back to the appropriate source within a matter of seconds. This redundancy gives technicians and administrators the ability to swap the device with a hot spare, pull the existing edge device out of service analyze what the problem was.

References

Fogarty, K. (2013, May 13). Server Virtualization: Top Five Security Concerns. Retrieved April 11, 2015, from http://www.cio.com/article/2428191/virtualization/server-virtualization--top-five-security-concerns.html

Humphries, D. (2014, August 1). BYOD Survey: How Are Employees Using Their Devices On Your Network? Retrieved April 12, 2015, from http://intelligent-defense.softwareadvice.com/byod-survey-employee-devices-your-network-0714/

Lyon, C., & Osterman, M. (2014). Security BYOD: Be Your Own Defense.*SIGUCCS '14,* 29-32.*

Microsoft. (2014, March 12). Border Gateway Protocol (BGP) Overview. Retrieved April 11, 2015, from https://technet.microsoft.com/en-us/library/dn614183.aspx

Roust, M. (2005, January 1). What is directory harvest attack (DHA)? - Definition from WhatIs.com. Retrieved April 11, 2015, from http://searchsecurity.techtarget.com/definition/directory-harvest-attack

Pearce, M., Zeadally, S., & Hunt, R. (2013). Virtualization: Issues, Security Threats, and Solutions. *ACM Computing Surveys (CSUR), 45*(2), 39-39.*

VMware. (2012, January 1). Controlling Virtual Machine Sprawl. Retrieved April 12, 2015, from http://www.vmware.com/files/pdf/techpaper/VMware-Controlling-Virtual-Machine-Sprawl.pdf