Tui itm 550 network administration assignment

ITM 550 MODULE FOUR CASE ASSIGNMENT 5 June 2011 Why do companies find it necessary to distinguish between network administration and systems administration? The first line of defense for almost every organization is typically the system administrator. This is the person that actively interacts with the company network on a daily basis, and by extension has intimate knowledge of it. So it stands to reason that this person would hopefully be the first to notice any signs of possible compromise would it not? Sadly that is often not the case.

Whether it is due to a lack of IT Training, complacency, or laziness is anyone’s guess. Several of the company networks that I have been involved with have the same story. All of them have been compromised by exploits, which have been out in the wild for some time. In other words a patch for the exploit has been released and is available. Why then did the system administrator not go out and download then install this patch? Surely it cannot be ignorance? A system administrator is a knowledgeable person who has specialized knowledge.

If they can successfully administer a large LAN composed of hundreds of users and a dozen servers what is the issue then? I’m too busy! One possible issue is that the administrator is simply too busy. Though as I am sure they will admit it is easier to simply go to the vendor site and get the patch then it is to rebuild an entire machine. This is especially so if it is one of your critical servers. That also begs the question of: does the sys admin regularly check that the backups actually work? Should the worst happen and you are compromised does your backup actually have what it is supposed to have?

Nothing is worse then finding out your backup plan actually doesn’t work. Rather imperative I would think that you would need to verify the integrity of your restoration media. Few and far between are the admins that actually do check their backups in my experience. An unacceptable lapse indeed, but a reality nonetheless. A key theme that I have been building upon here is that a lot of responsibility lies upon the shoulders of the admin. All too often though for a variety of reasons the admin comes up lacking. What do you do then to remedy that situation? For me it would be an easy fix.

How about building in accountability into the system administrator’s job description when they sign on with you? This to me would be the simplest solution, as it would force accountability upon the admin. Not only that but you also hold a hammer over their heads should they not perform their duties as expected. After all this isn’t kindergarten anymore, and we all have duties to discharge with an expected level of professionalism. Is the admin really to blame? So we have a problem in that time and again the system administrator has been proven to be at fault.

Not only at fault but, on a matter so centric to their jobs that it really does boggle the mind. Why didn’t they download that vendor patch! Anyone can harp about a problem, however it is preferred if one also gives a possible solution. With that in mind, this is how I would go about ensuring that my front line people are indeed doing their jobs properly. After all, patching the operating system you are running is very much a system administration job. Once a suitable candidate has been found for your vacant system administrator position you need to go over their list of duties.

This is something that needs to be written down on paper so that later on there is no room for misunderstanding. Included in this job description is that they will check the vendor site on a daily basis for any patches, or other operating system information. The same should be included for any other third party applications they will need to maintain. All said and done that is an excellent policy to have, and furthermore is one many companies have. So why then do we keep seeing these very same companies having problems with old exploits? Human nature, being what it is, laziness creeps in, and the vendor site is no longer being checked.

That or a box is rebuilt and the sys admin puts it back on the network with no patches, as they will install them in a second or two. If I had a nickel… I don’t know how many times I have heard this when the admin in charge is queried after the fact while an incident is investigated. “ Geez it was only on the network for a minute or two! ” No one really expects the sys admin to be a security guru but certain fundamental practices must be observed. One of those is to have all those patches on a cdrom so that the rebuilt machine can be patched offline.

Much like the admin checking on a daily basis for newly released system patches. It’s just good business after all. So to wrap up all of the above verbiage, what should one do to ensure the sys admin is staying on top of patches? Well simply put, I would have a sheet where the sys admin would need to sign off on. That person’s signature would attest to their having verified the vendor site for patches each and every day. Not only that but I would personally have them checking out the mailing lists as well on a daily

basis. This would help give them situational awareness as it impacts them and their network.

With that in mind if the sys admin has indeed signed off on that sheet and the company is compromised because of an old exploit then the answer is simple. You’re fired! Many system administrators out there may find this rather harsh. The reality of it is that there is little to no accountability for system administration. Unless the step of having the new network admin sign a job description has been taken, there is precious little in the way of known punitive steps management can take. In many companies it would still be considered a firing offence for having forgotten, or outright neglected to patch company servers.

There are many good admins out there today, but a great deal more need to become far more proactive in their duties. One of the most vital ones being to keep the software up to date patch wise. Parker (2005) A network administrator is a person responsible for the maintenance of computer hardware and software that comprises a computer network. This normally includes deploying, configuring, maintaining and monitoring active network equipment. The network administrator (or “ network admin”) is usually the level of technical/network staff in an organization and will rarely be involved with direct user support.

The network administrator will concentrate on the overall integrity of the network, server deployment, security, and ensuring that the network connectivity throughout a company’s LAN/WAN infrastructure is on par with technical considerations at the network level of an organization’s hierarchy.

Network administrators are considered tier 3 support personnel that only work on break/fix issues that could not be resolved at the tier 1 (helpdesk) or tier 2 (desktop/network technician) levels. Depending on the company, the Network Administrator may also design and deploy networks.

The actual role of the Network Administrator will vary from company to company, but will commonly include activities and tasks such as network address assignment, assignment of routing protocols and routing table configuration as well as configuration of authentication and authorization – directory services. It often includes maintenance of network facilities in individual machines, such as drivers and settings of personal computers as well as printers and such. It sometimes also includes maintenance of certain network servers: file servers, VPN gateways, intrusion detection systems, etc.

Network Administrators may also be technically involved in the maintenance and administration of Server, desktop, printers, routers, switches, firewalls, phones, PDA’s, application deployment, security updates and patches as well as a vast array of additional technologies inclusive of both hardware and software. The administrator is responsible for the security of the network and for assigning IP addresses to the devices connected to the networks. Assigning IP addresses gives the subnet administrator some control over the personnel who connect to the subnet.

It also helps ensure that the administrator knows each system that is connected and who is personally responsible for the system. Duties of a Network Administrator Many organizations use a three-tier support staff

solution, with tier one (help desk) personnel handling the initial calls, tier two (technicians and pc support analysts) and tier three (network administrators). Most of those organizations follow a fixed staffing ratio, and being a network administrator is either the top job, or next to top job, within the technical support department.

Network administrators are responsible for making sure that the computer hardware and network infrastructure for an IT organization is properly maintained. They are deeply involved in the procurement of new hardware (For example: Does it meet existing standardization requirements? Does it do the job required?), rolling out new software installs, maintaining the disk images for new computer installs (usually by having a standardized OS and application install), making sure that licenses are paid for and up to date for software that need it, aintaining the standards for server installations and applications, and monitoring the performance of the network, checking for security breaches, poor data management practices and more. Most network administrator positions require a breadth of technical knowledge and the ability to learn the ins and outs of new networking and server software packages quickly. While designing and drafting a network is usually the job of a network engineer, many organizations roll that function into a network administrator position as well. One of the chief jobs of a network administrator is connectivity.

Network administrators are in charge of making sure that connectivity works for all users in their organization, and for making sure that data security for connections to the Internet is properly handled. (For network administrators doing security aspects, this can be a full time job.) Trouble tickets work their

way through the help desk, then through the analyst level support, before reaching the network administrator’s level. As a result, in their day-to-day operations, network administrators should not be dealing directly with end users as a routine function.

Most of their jobs should be on scheduling and implementing routine maintenance tasks, updating disaster prevention programs, making sure that network backups are run and doing test restores to make sure that those restores are sound. Wikipedia (2011) Bibliography: Parker, DP. (2005, July 21). System adminstrator friend or foe. Retrieved from http://www. windowsecurity. com/articles/Sys-Admin-Friend-Foe. html Wikipedia. (2011, May 27). Network administrator. Retrieved from http://en. wikipedia. org/wiki/Network_administrator