Identifying potential risk, response, recovery

In this paper I have just been hired as an Information Security Engineer for a video game development company. I have previously identified all of the potential Threats, Vulnerabilities and Malicious Attacks for the videogame development company. The CIO have reviewed my report and has now requested that I draft a report analyzing and assessing any potential Malicious Attacks, Vulnerabilities and Threats that may be carried out against the company's network. I will then choose a strategy for dealing with risk, such as mitigation, assignment, risk and avoidance.

Next I will develop controls that will be used to mitigate each risk. Now let's begin by discussing the threat of the Web/FTP server, some servers, or hosts, must be open to the internet. Web servers are examples of such hosts. You want any user to be able to access your web server- but you don't want everyone to be able to get to your internal network (Fundamentals of Information Systems Security). The simple solution for this is just to isolate the host that is connected to the internet from the internal networks and then create a demilitarized zone.

The risk mitigation for the Web/FTP, the FTP is very useful for working with remote systems, or to move files between systems. On the other hand the use of FTP across the internet or other untrusted networks, exposes you to certain security risk. Your object authority scheme might not provide enough protection when you allow the FTP on your system. The next risk for FTP is a hacker can mount a denial of service attack with your FTP server to disable user profile (FTP Security). This is usually done by repeatedly trying to logging on with the incorrect password for a user profile, generally until the profile is disabled.

This kind of attack will disable the profile if it reached the maximum sign on count of three. If the company use a FTP server logon exit program to reject logon requests by any system user profile and those user profiles that the company designate will not be allowed FTP access. Now we will discuss the NIDS, the primary purpose of a network-based intrusion detection system is to identify attackers trying to expose vulnerable network services. The NIDS can respond to the attack or alert personnel, who can take the necessary and appropriate actions for this type of attack.

NIDS allows administrator to respond to attacks with actions appropriate to their security policy. To properly analyze false alarm reduction strategies, it is necessary to quantify risk and the NIDS role in risk reduction. The NIDS uses two formulas, one formula assumes that risk is roughly equivalent to single loss expectancy. This formula for this quantification is SLE= (Asset Value x Exposure Factor) (Fundamentals of Information Systems Security). The next formula states that risk is equal to exposure multiplied by threat. Risk= Exposure x Threat.

This equation determines threat and the type of threat. For example there are threats of port scans, automated scans and sweeps, Denial of Service and Service attacks and compromises. Now we will move on to Windows 2008 Active Directory Domain Controllers (DC), because domain controllers provide critical services to their clients, it is crucial to minimize the risk of any disruption of these services that may be caused by malicious attacks. Antivirus Software can be used to mitigate the risk of malicious attacks in Windows 2008 Active Directory Domain Controllers.

Make sure that you verify the antivirus software you select is confirmed to be compatible with your domain controllers. Do not use domain controller systems as general workstations. Another way to prevent malicious attacks on domain controller systems is to not allow users to use domain controllers to surf the web or to perform any other activities that can allow the introduction of malicious code. Only allow browsing on sites that are known to be safe, this will be did strictly for the purpose of supporting server operation and maintenance.

Another practice to keep in mind is to make sure that all of the company's files, including the shared ones, should be ran against a virus scanning software. This bring me to the file servers, have the potential to receive different viruses such as worms, Trojan horses and logic bombs. To allow an end user to upload files to your website, is like opening another door for a malicious user to compromise your server (acunetix. com). File uploads are permitted in social network applications. File uploads are also allowed with blogging, e-banking sites and you tube.

All of these network sites allow users the opportunity to efficiently share files with corporate employees. Users are allowed to share files with corporate employees, through uploaded videos, pictures, avatars and many other types of files. The best way to prevent malicious attacks through the company's file servers is to make sure that the file that is being uploaded is validated. This will prevent a hacker from uploading files with malicious codes that can lead to a server compromise. Another way to prevent a malicious attack on the file server is for the company to block all dangerous extensions.

In cases like this, there would be a blacklist, the list will show the dangerous extensions and there access will be denied if the extension of file they are trying to upload is on this list. The best practices to follow when uploading files onto websites and web applications. The first risk mitigation in a file server is to estimate the size of programs, files, and transaction. Then you will need to prevent deviation in size of the files as well as the amount of users that have access to the files. Now we will move forward the Wireless access point (WAP), this is the connection between a wired and wireless network.

This is also a wireless security protocol designed to address and fix the known security issues in WEP. WAP’s are radios, sending and receiving networking information over the air between wireless devices and the wired network wireless (Fundamentals of Information Systems Security). The best way to prevent malicious attacks on a WAP is to increase security. Presently WPA provides users with a higher level of assurance that their data will remain protected by using Temporal Key Integrity Protocol for data encryption.

If the data is not encrypted then it is considered as fair game, because it would be very easy for anyone that have access to a radio to access this data. The mitigation risk for a Wireless access point is to make sure yourtechnologyis updated. Failureto upgrade to newer, more advanced technologies could potentially impact productivity and lead to significant downtime, security vulnerabilities, and non-compliance issues. Older wireless technology do not support new features and functions that are proving to be so valuable.

Next you will need to choose the right carrier, ensuring information is secure within the supply chain, complying with all the latest government and retailer mandates and taking advantage of all the latest features and functions to save time andmoneycan seem like a daunting task (Wireless technology Migration: Mitigating risk and increasing supply chain efficiency). Now we will discuss the 100- Desktop/Laptop computers, both of these computers are subject to viruses such as worms, hoaxes, Trojans and other security vulnerabilities.

The best way to prevent these from occurring is to install and use a firewall. Always make sure you are installing and updating the latest critical security software. Add a virus software scanner, to allow the software to scan your computer for potential viruses. Next we will discuss the VOIP telephone system, this is one of the newest technologies that is being rapidly embraced by the market as an alternative to the traditional public switched telephone network. The malicious attacks that can occur with this system is denial of service, impersonation or spoofing or toll fraud.

The best way to prevent this from happening is to add port security, cisco secure access control server, DHCP Snooping, Cisco firewall solutions and intrusion prevention. Data transit can also be used to protect the voice traffic over the wireless LAN’s. The risk mitigation for desktop/laptop is as followed is to target malware with automated defenses. One of the first line of defenses for any PC or laptop is to block or eliminate viruses, worms, spyware, and other malware, including Trojan downloaders and keystroke loggers, both on endpoints and at the gateway.

Deploy anti-malware and filtering software for all email gateways, to prevent malware and spam from ever reaching the PC’s. Next you would want to patch your vulnerabilities as quickly as possible, create a password to access your PC or laptop. To really maximize security in a minimal amount of time, as part of the “ acceptable use” policy, prohibit users from installing unauthorized software on PC’s or laptops (10 Ways to mitigate your security risk).