Cybersecurity Investigations and laws

CS 698

Assignment 1

Hawk eyes: **Adhithya Sivanesh (as3423), Gautam Pandey (gp88), Ketaki kakade (kk524)**

Taking into consideration the entry and exit points of a network which could be vulnerable to attacks and which may compromise the integrity of a company we have come up with the following constraints of the network. The paper also suggests security measures that should be taken in order to protect the intranet and internet of the company.

Secure access points to the company networks

This phase is one of the important aspects that must be taken care of in any organization. If these points allow only authorized officials to have access, then breaches and other targeted attacks could be stopped at its initial state itself. This security mechanism allows an organization to actively defend itself at every possible connection in order to prevent any future intrusions or attacks that could affect the smooth functioning of the organization.

These access points could be within the network or outside the network, for example, the access points between servers, databases, user devices, access hubs within networks, network applications(web, email) etc. There must be a distributed detection and response technologies at each access points. These could be taken care of by implementing firewalls in a customized fashion that serves our need along with high standards of security. The perimeter build by firewalls could be then extended outward to remote locations by using encrypted tunnels.

Vulnerability assessment and penetration testing (VAPT and Security audit)

An organization could be a combination of several networks, applications, web pages, servers etc. Once these entities are up and functioning, the next important aspect of security is to make sure that they are not penetrable or could not be compromised. This could be done by carrying out regularly timed vulnerability assessment and penetration testing of the different assets of the organization. Make sure each of these assets are updated and patched at regular intervals.

Reports are supposed to be made based on the findings of the testing, and these reports need to be submitted to the executive team as well as the technical team so that necessary actions could be taken. Usually these reports scale the vulnerabilities found on different assets on the basis of high, medium or low, and also should involve the necessary steps that must be taken so that these vulnerabilities are not used into advantage by any attacker.

Management of logs

A log is a record of the events occurring within an organization's systems and networks. The log data could be very useful to detect any intrusions from within or outside the network. These logs could also be used for troubleshooting as well as identifying the reason for any system or hardware failure. The IT team could use a log manager tool that would help them to interpret, read and respond to the data stored in the log files.

Whenever the system is compromised or a breach occurs, the logs are the first thing that the forensic team would require as it contains the complete digital footprint of what was happening in the network.

The usage of logs could also help a system or network to recover from threats. The logs need to be surveyed at regular intervals to increase the secure functioning of the organization. Based on the log activity necessary steps could be taken in order to maintain security.

Mitigation strategy

The best and simplest strategy for recovering from an attack is to make sure the affected part is isolated and to be sure that the attacker could not possibly make his way into other regions within the network. Pinpointing the affected region and blocking the attacker access to other sectors could be time consuming depending on the scenario, and if not handled quickly things could go even worse. So one of the primary step that would make this mechanism less time consuming is to be proactive and block any intrusion of any sort with quick response.

Since an organization could deal with data of different forms and even third party information, so it is the responsibility of the organization to make sure that these data are kept safe in such a way that even if these data gets corrupt or compromised, there must be a recovery mechanism in place that could help the smooth functioning of the organization. This could be done by making use of regular backup of all the data it is dealing with, or could make use of cloud services for storing data as backup.

The network could make use of honeypots that could be used to lure cyber-attacks, detect, deflect or study attempts to gain unauthorized access to information systems, because any activity related to the honeypot is considered as malicious since, a normal user would never stumble at this level. This honeypot could be something that resembles the normal functioning of a system in order to trap the attacker.

The system must maintain Intrusion detection system (IDS) and Intrusion prevention system (IPS) as these could be considered as the outermost layer of security to prevent any unwanted intrusion into the system.

Cloud

There has been a drastic change in the field of data storage and processing, a number of companies that do not have the necessary resources to store and process their data securely and efficiently, can cross this off from their list now as the cloud provides an efficient and economical alternative.

There is however a very severe issue that needs to be discussed here, cloud computing requires the organization to connect to the cloud through the internet which may not always be secure. To add to the worries, is the fact that data is being transferred through these connections that are partially insecure to say the least.

This can expose highly valuable data and intellectual property of the organization. There could be cases where the data is unencrypted at the source due to the sheer volume and velocity of streaming data and lack of resources to handle this volume of data.

There have been cases where the unencrypted data has been captured on the fly from source to destination. One such example was the TJX Group incident where TJ Maxx and Marshalls stores, brands owned by TJX Group was sending unencrypted data packets were being sent on the fly to the destinations which would process approve or reject the transaction on this basis. These data packets were captured by a third party using packet sniffers and more than 45 million credit card details were compromised.

So proper encryption at source is very necessary when working with a cloud based setup. It is the responsibility of the organization to ensure this.

Servers and Datacenters

Almost all businesses in this day and age are switching towards data driven solutions like Recommendation engines,Real time analysis of transactional data to provide business insights and suggest measures to optimize the business. The most important factor in all of these solutions is data. It is critical that we can store our data securely and aid in the efficient processing of this data.

There are several threats that we deal with Servers and Datacenters in regards to the security, two of the more exposed vulnerabilities are Denial of Service attacks and encryption techniques that are not capable to defend against brute force attacks coupled with superior hardware and expertize.To add to the problems the amount of data generated is also increasing rapidly and

some of the legacy systems which are still in use simply were not designed to handle this amount of number crunching.

Solutions to these problems depend on the size and financial capacity of the business.

The businesses who do not have the capacity and infrastructure to meet the threat which is rising exponentially because of the increased capabilities of modern attackers with just commodity hardware. The most cost effective and robust solution for these organizations is moving to the cloud where none of this is now your responsibility except for data at the source which is limited and can be secured with the existing infrastructure.

Some businesses however, can not afford to compromise their data as the financial liability associated with the data far exceeds the cost of setting up a secure infrastructure. This is the main reason they do not trust the cloud to secure this data and take it upon themselves to implement high levels of security.
The other issue is that in the modern day you need real time processing of huge streams of data that is being generated by the second. In case of the cloud architecture network which is now the internet, acts as a major overhead and could significantly slow down the entire process. For this reason big companies which rely on business intelligence and data driven solutions are reluctant to shift to the cloud.

The solution for such organizations is to create their own infrastructure which is highly secure and can also optimize data processing. Strong Firewalls must be implemented, there are various companies who specialize in cybersecurity solutions to handle various use cases in the field of security such as Fireeye. Third party products must be looked into can be deployed and optimized by the cybersecurity company to fit your requirements.

Third Party involvement

There are often teams within an organization that use third party services or solutions to execute certain tasks, this poses a security threat as you are now sharing data with a third party and this may not be best approach considering that some of these third party applications are not very secure. One way to minimize this threat would be to only approve trusted third party services or solutions which are secure and follow the most updated security protocols. An alternate approach could be to build on top of a third party service and add your own layers of security.

Potential losses

There can be a ton of security measures but that does not mean that organizations are always secure, as attackers find new techniques on a regular basis.

It is best to prepare for the worst, which in this case let us assume would be a data breach. So now you have a data breach and you may not be insured to cover the amount associated with the data breach.
This can result in heavy losses. To avoid this situation, we should have a fair and unbiased inspection of the vulnerability and calculate the total liability in the worst case scenario.. The whole process needs to repeated periodically to get an accurate amount. This is the amount that we should roughly be insured for.

Access control

Loss of intellectual property is one of the biggest risks facing companies with limited controls on access mangement. To limit the chances of sensitive information falling into the wrong hands, most companies have identity access management (IAM) systems assigned to their IT networks. Without access management restriction in place, sensitive information, with or without protection, could easily be leaked to a rival organization or to the hacker.
policies should be laid down in order to maintain adequate level of security to protect data and information systems from unauthorized access.This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of information systems. This policy affects all employees of the company and its subsidiaries, and all contractors, consultants, temporary employees and business partners.

Workstation Access Control System: All workstations used for the company business activity, no matter where they are located, must use an access control system approved by the company. In most cases this will involve password-enabled screen-savers with a time-out-after-no-activity feature and a power on password for the CPU and BIOs. Active workstations should not to be left unattended for prolonged periods of time.

System Access Controls: Access controls should be applied to all computer-resident information based on its' Data Classification to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.
Access Approval: System access should not be granted to any user without appropriate approval. Management should be immediately notified about the Security Administrator and report all significant changes in end-user duties or employment status. User access should be immediately revoked if the individual has been terminated. In addition, user privileges should be appropriately changed if the user is transferred to a different job.
Remote access: Any User (remote), accessing the company networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes but is not limited to:

- Automatic logoff

• And Unique user identifier
• At least one of the following:
• Biometric identification
• Password
• Personal identification number
• A telephone callback procedure
• Token

Multiple-factor of authentication must be provided in which remote user requires two or more forms of verifications in exchange of access to internal network. Example, the user needs to go through a basic password authentication and then an passcode is sent to the user to his cell phone or an email is sent in order to verify the user.

Training employees for defending against social engineering

Human error and negligence play a major role in cyber security breaches. Despite the money spent for security, the simple social engineering tactics prove effective in compromising the employee vulnerability. Those in charge of IT security must consider the possibility of such attacks and prepare for them accordingly. The prevention plan should include educating employees on social engineering attacks.

Employees should be educated for the following :

1. Phishing Emails

There are multiple forms of phishing attacks to avoid, including spear phishing and whaling. prevention or human error in perhaps a potentially egregious incident or breach.Basic phishing awareness may entail paying attention URLs included in organization emails, not clicking on links from external emails, not opening attachments unless allowed to do so in an internal email, and never engaging with requests to provide email or other passwords from internal or external sources unless you requested it. If a person opens an attachment they could activate malicious software unknowingly, which could easily give an unwarranted party access to the local workstation and internal network.

2. Phone Scams

False Tech Support Calls

Phone scammers are notorious for fake Windows support calls. They used to call to help employees or personal users with issues, ask to remote into their desktop. Then they would secretly install malware and extort money from the user for removing it.

In my current position, I work with several different third-party software systems. When problems arise there are times to contact their technical support. It’s smart to have a healthy dose

of skepticism when speaking with technical support representatives over the phone or email. Do not give out passwords, answers to security questions, anything personally identifiable.

Screen Phone Calls

Phone scammers are highly effective. Rather than engage with anyone who calls your extension and states your name and position, go on the offensive. Never readily admit your identity on an unfamiliar incoming call. Ask for their contact information and to leave a message. Phone scammers will usually leave false contact information and move on to the next target when faced with an obstacle.This phone awareness should apply to everyone in the organization, especially secretaries and other personnel who are the first line of defense with main line calls. If the incoming call does not know their party's immediate extension, do not transfer the call.

Password Policy

Employees should be educated in regards of setting and storage of their passwords. Passwords should not be stored in readable form without access control or in other locations where unauthorized persons might discover them. All such passwords are to be strictly controlled using either physical security or computer security controls. All programs, including third party purchased software and applications developed internally by the company must be password protected.

The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. After three unsuccessful attempts to enter a password, the involved user-ID must be either: (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than three minutes, or (c) if dial-up or other external network connections are involved, disconnected.