International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 05 Issue 01 | 2020

Insider Threats

[1]Priyadarshini Krupendra
[1]Master student, Department of MCA, PES University, Bengaluru, Karnataka, India

ABSTRACT

Insider threat is a dangerous threat where this comes from the people within the organization like employees, contractors, business associates, former employees and those are involved in the valid organizational information of security practices, data and computer systems. This may get involved in the fraud, theft, destroyed, of the valuable information in the systems. The topic comes in the 3 categories:
1. Malicious Insiders: The people who take advantages are the ones who get their access to harm an organization. 2. Negligent Insiders: The people who make errors and discard the policies and this keeps the organization at risk. 3. Infiltrators: these people are external person that get law of access without authorization. These inside threats are always pressing the issue of both domestically and internationally. There is news about these kinds of threads frequently coming up and the future research analysis is very important. These helps in the company to take more precautionary measures of increasing much security features that help the company to identify these types of characteristics and behaviours and give them motivation. To make this perfect the companies need to take more hands-on, fast approach for the company-wide involvement.

Keywords:Insiders, Threat, Characteristics, Behaviours, Approach, Pressing, Risk

1. INTRODUCTION TO NETWORK SECURITY

Network security is basically the prevention and protection of the network against the unauthorized private space. This helps to improve the endpoint security and focuses on individual devices. The network security also focuses on the device's interaction with the network and the bond working background behind it and the connectivity between them. This network security is taking measures of the organization very seriously by protecting physical and software networking infrastructure from unauthorized hands or devices. This helps in creating the secured platform for computers, users, and programs to perform on their permitted functions within a secured surrounding. The overall trust will be the same. There are multiple tasks.

1.1 Network security basics

This defines that the lay of plan are intended to be implemented to the top-level statements of vision. This of basics of the network security are there over a decade for CSOnline. This strongly intents to three phases of NS and are very important and are still on recommendation of using for the underlying framework for their own strategy. These contains:

- **Protection**: You should be able to configure the systems and networks as perfect as possible of the recommended.
- **Detection**: The one must be able to identify the configuration that has been changed, whenever the network trafficking indicates a problem.
- **Reaction:** After identification of the problem the one must respond and return them to a safe state immediatelytools which can be used to prevent from unauthorized to get connected to it.

Fig1: Network Security

1.2 Network security methods

To make of these define, there are multiple of preferred techniques and types of network security. The below are the some of the preferred ways to attack and safeguard the organization and these are also in action in many companies to secure their networks.

- **Access control:** The one should be able to block the users and devices unknown from accessing the network to the organization.
- **Anti-malware:** There are different kinds of malwares that can spread across the network like virus, worms, Trojans etc., this can get into the network and harm the machines within a week. It all depends on how strong or best the security one has maintained to not infect the network.
- **Application security:** The main is to protect the applications where those are the leaked path for the attackers to get access to the network. The one must keep track of the hardware, software and security to lock down for the better safety.
- **Email security:** This is the most common happenings in today world basically Phishing. This help in easy access to the attackers and one should be clean and educated about the incoming attacks and outbound messages having sensitive data.
- **Firewalls:** This is the big daddy of the NS, where they follow rules to permit and deny the traffic from the start between the network and the internet. This trusted zone help give access to the known devices and keep the defensive attack till it has been deactivated.
- **VPN:** This tool is basically a contact between the device and secured network, and this creates a big channel for secured, encrypted data across the open internet.

2. NETWORK SECURITY AND THE CLOUD

The enterprises are few times into the offline loading of their data I to the cloud Providers. These internal networking has a been seemingly and secured with the hosted third party. This few time is a majorly self-contained network which can be either physical or virtual with the requirements of the networking of their dependency.

To handle some of the security aspects of the organizational demands various vendors are being established. This can help ease some of their worries and the truth is there are few loopholes, but the security of that organization may cover up the holes and provide a super cloud network security.

Cloud computing is the most trending in recent days because of its flexibility and support. It allows us to access personal and shared resources with minimal management. It sometimes relies on the internet. There are many third-party cloud services available in the market which saves expanding resources and maintenance. Most appropriate example of Cloud computing is Amazon Elastic Cloud Compute (EC2), which is highly capable, low cost and flexible.

Major characteristics of cloud computing include:

- On-demand self-service
- Distributed Storage
- Rapid Elasticity
- Measured Services
- Automated Management
- Virtualization

Cloud computing is the availability of computer resources like data storage and computing power. The term is often used to describe data centres available to many users over the internet. One of the important features of cloud is functions distributed from central servers over multiple locations. Cloud computing types are service deployment models that allows us to choose the level of control over our information and the types of services we need to provide.

2.1 Types of Cloud Computing Services

The three main types of cloud computing services are:

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

2.1.1 Infrastructure-as-a-Service (IaaS)

Infrastructure as a service (IaaS) can be defined as a cloud computing model that allocates virtualized computing resources to the user through the internet. One of the main components of cloud computing is IaaS. IaaS is completely monitored and managed over the internet.

The IaaS technology helps the users to save the cost and manage their own physical servers by reducing complexity. All the resources of IaaS are offered as individual service components and the users select them depending on the need. The users are supposed to concentrate on installing, configuring and managing the software while the cloud service provider manages the IaaS infrastructure.

2.1.2 Platform-as-a-Service (PaaS)

PaaS is another type of cloud computing model in which a provider from third-party delivers hardware and software tools over the internet which are used in application development. Hardware and software are hosted on its own infrastructure by the PaaS provider. As a result, there is no need for developers to install in-house hardware and software to develop or run a new application. There is no need for PaaS to replace company's entire IT infrastructure for software development. The users most frequently access the offerings through a web browser, which is provided through a cloud service provider's hosted infrastructure. PaaS is sometimes delivered through public, private and hybrid clouds to deliver services like Java development and application hosting.

2.1.3 Software-as-a-Service (SaaS)

The third cloud computing type is SaaS which is used for web-based applications. SaaS delivers software applications over the internet. Cloud providers host and manage these applications by making it easier to access the same application on all of our devices at once from the cloud.SaaS applications are usually accessed by users using a thin client such a web browser.

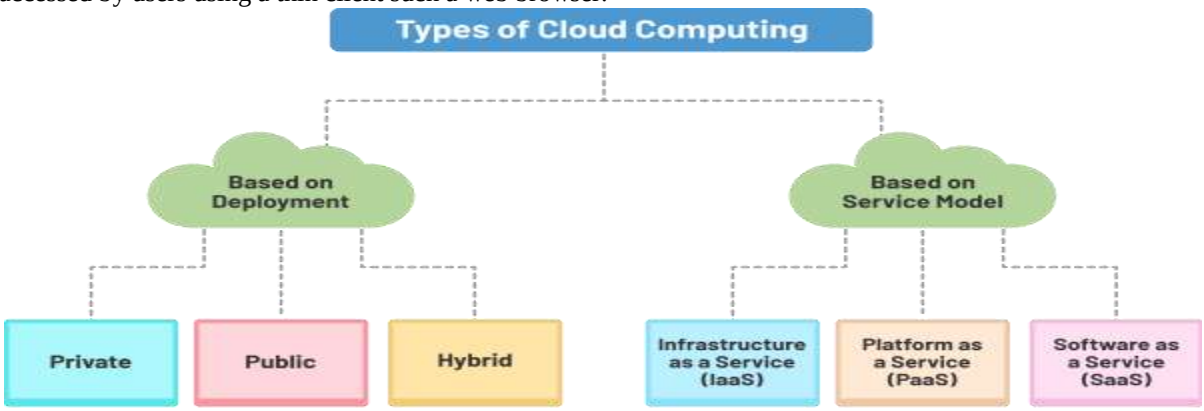

Fig-2: Types of Cloud Computing

2.2 Types of Cloud Deployments

2.2.1 Public cloud

Public cloud is usually offered by SaaS to users over the internet. It is one of the most economical options for users where the service provider bears the bandwidth and infrastructure expenses. The cost is determined by usage capacity. It has limited configurations due to its lack of SLA specifications. Public cloud is not the best choice for organizations with sensitive information as it compromises data and breaks security regulations. Some of the features of public cloud are high reliability, lower costs and zero maintenance.

2.2.2 Private cloud

Large organizations use private cloud to build and manage their own data centres business and IT operations. The private cloud provides control over scalability and flexibility to improve security of assets and business operations. Private cloud can maintain hardware and software environment over a private network. Government agencies and Large and Medium-scale financial enterprises usually go for private clouds.

2.2.3 Hybrid cloud

Hybrid cloud is the combination of private and public cloud, which provides more flexibility to businesses having control over critical operations and assets. Hybrid cloud enables companies to take advantage of public cloud when necessary due to their workload migration. For example, public cloud is used to run high-volume applications like emails, and they utilize private clouds for sensitive assets like financials and data recovery.

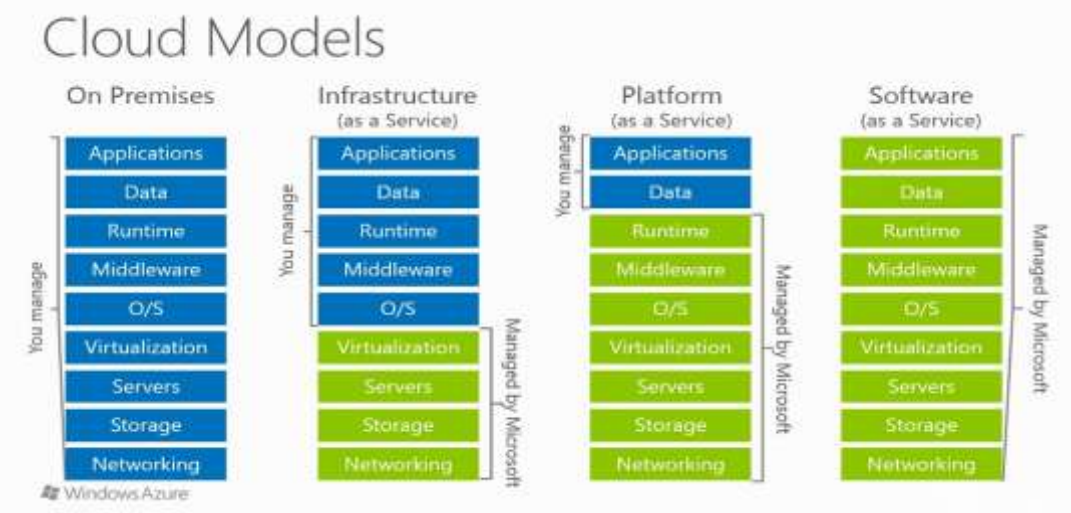

Fig-2: Cloud Models

3. INTRODUCTION TO INSIDER THREATS

Insiders would be having an account to get access to the computer systems of the organization and this access helps them to get easy access to the servers to perform their duties, where these permissions are being misused to harm the organization. Insiders always keeps track of the organization data and their property of methods that will protect them. The insider's treats are more dangerous because they can easily get the required data because they are already inside and it's difficult to identify also compared to outsider. An insider can steal the required data for personal benefits. They steal from an organization and sell this to market to gain transactions or they start blackmailing the organization.

Organizations are spending huge amount of money for their security purpose to protect against the outsider called hackers. But there are more serious issues they must solve inside the companies itself and they are the once who are more dangerous than the outsiders. They would have already got the access to the servers before itself so the detection inside the organization is very must. Even though the companies are trying to cut down the insiders the frequency of them are growing much faster every year.

The things of few statistics show about the harm that the organizations are facing. These attacks are considered as the most treats than the outsiders' threats or attacks. The insider do not only cause damage to the company information or data but this is a shameful act by the physical and the reputation of the organization goes down and this also effects the company's financial status also so this is called logic bomb where an ex-employee plants the bomb inside the information and when he is removed the bomb explodes and the whole information is being lost.

The more concerning is that the thoughts of insiders working for a government facility dealing with the materials that can cause such a destructive unavoidable impact. There are still more companies who are still not prepared for the insider's attack and lack of understanding of these insiders' types are being at loss all the time. The company has to take up some of the actions by identifying the character and behaviours of the insiders, motivations, this can help the companies take up the preventive methods and keep their company away from such threads. The working definition of an insider threat must be developed at first using few normal present technologies, as this can be very helpful for everyone throughout the world.

Fig-2: Insider Threats

4. Managing the Risk of Insider Threats

Believed Risk management framework and the policy to which it has been managed by the Risk of the insider threads does not draw breath. Risk is defined as (probability of an event) times (consequences of the event). We know little about either. The impact of insider threats can occur in multiple dimensions: financial loss, disruption to the organization, loss of reputation, and long-term impacts on organizational culture. These impacts can be highly nuanced and are not well measured or accounted for. For example, "bonus round" insider threats (actions taken in anger, revenge, spite regarding bonuses, compensation) can have severe consequences on all levels of an organization. Thus, a rather small or illogical motivation can have a vast influence. Equally, the effect may not depend on motivation – an innocent act can have a destruction impact as a maliciously motivated attack. The goal is to keep away the catastrophic consequences regardless of the motivation. These aspects and other risk catalyst should be represented in threat would to be accepted as of their importance. It seems reasonable to assume that the probability of different types of insider threats will vary across organizations and circumstances. Little concrete can be said about this. At last, this has been unclear that how effective a various prevention, detection, and the responds techniques are being in reduction in the insider threat and this helps in the reduction of the risk as well. For example, we may lack any of the précised data to specify how effective the different security policies are being dependent on the motivation of the insider. It may be that this does not matter; anecdotally it appears that sometimes it is hard to distinguish the execution and consequences of malicious acts from those due to accidents. On the other hand, it may be an appreciable deal. Insiders may lawfully use domains in different ways which may trigger flawed alarms. Outsiders acting with illegitimately acquired credentials, insiders acting with malicious intent, insiders acting without malicious intent, and accidental behaviour are all insider threats, and yet it remains unclear how constructive various security rules are opposed to acts stemming from other influencers.

The risk of insider threats are the threats or risks occurred in an organisation. They can occur severely in all kinds of dimensions they vary based on the circumstances and consequences faced during the organization therefore, to avoid these threats motivation may play a major role in reducing risks. These insiders are disastrous to the company and can lead to small or big risks. There are no proper elements to reduce these insider risks and there are domains which can be used in a different way which leads to huge risk in the organization and it is unclear how the policies and consequences are against these insiders.

5. Insider Threats Requires Technical Approaches

The first area is to be considered as a technical approach. These include the means to execute, observe and reduce insider threats.

Policy Languages:
Policy languages can be used to generate human-readable interpretation. The biggest concern is their offensiveness and demonstrativeness. The policy regulates the important aspects of the company and these formal policy languages is important when organizations unite, and the respective policies are to be adapted.

Access Control:
Access control is a way of dealing with insider attacks. This grants the user an advantage to execute the required tasks according to the rules set by the organization. Access controls are the mechanism which supplies electronic resources based on credentials. Role-Based Access Control (RBAC) is finer-grained approach. Limiting lawful access can have a gloomy effect on the productivity.

Monitoring:
Research says that harmful insiders operating can be recognized by noticing the pattern of information used. Anomaly detection flags significant divergence from expected behaviour as representative for unknown types of anomalous misuse. Monitoring can be done at the host level or network layer or both. Host sensors are harder to install than network sensors. Monitoring is useful in verifying a suspected insider attack.

6. Insider Threats Require Multiple Approaches

- Most incidents required a technical experience,
- Actions were already planned,
- Motivation was a financially secure,
- Acts were performed on the job, and
- Incidents were usually discovered by non-security personnel and by set of instructions

Insiders have a special knowledge of the organization than the outsiders, the interaction between the security policy and organizational dynamics is important in reducing threats. Managing and understanding the organizational realities is a variation and difficult in developing policies.

Each relative success of technical v/s non-technical approach varies:

- Misuse of Access: The insider has a certain privilege which misuses the system resources. This is the hardest form of attack to discover by technical means.
- Bypassing Defenses: Insiders are already inside the perimeter, and therefore have more opportunity for mischief. Reliance on technical or non-technical discovery of anomalous behavior or actual attacks is required.
- Access –Controller Failure: Insider should not have access to a resource. This is a technical problem and prevention is effortless, locating of access-control failures is difficult for same reason.

The insider threats are a name which covers varieties of threats altogether.

7. CONCLUSION

The main purpose of this paper is to discuss about the largely growing headache and the way the organization to tackle this insider and if any attack happens the measures to be taken cautiously without loss of data. The importance and education of this is must for an organization where it deals with every individual behaviour or the company employees. This helps in prevention of not compromising with the company's assets.

These insider threats have may forms and technical approaches tend to seek access control over many of the systems which have file structure intended to accidental or malicious activities by the insider. These contain the few organizational behaviour,sociology, psychology, and the treats motivations, predictions of the attackers, changes inside the structure, cultures, self-claiming, are the few signs to look out for inside the insiders. Outside attacks are hard to find but there are few things like tools to find out those things but in this insider are very much hard to by using the tools too so the organization should be very careful about these incidents. The importance should be given to the preventive measures of security than the reactive measures.

Therefore, the organization has to set-up the best security and look-out for the best behavioural content inside the employee.

8. ACKNOWLEDGEMENT

I am sincerely thankful to PES University for providing me with the opportunity to write a research paper on this topic. I'm also thankful to Mr Srinivas P, Assistant Professor for guiding me in every single stage of this research paper and supporting throughout the process in preparing a meaningful paper. I am also thankful to Dr Veena S (Head of MCA-CS& IT) of PES University who have helped me during this research paper in different ways. Through this paper, I have learnt how Network security & Insider threat functions work in different platforms. It has helped me toanalyse how the Network can be secured and prevented in different ways and its advantages and disadvantages.

9. REFERENCES

[1] "The CERT Insider Threat Centre". Cert.org. Retrieved 2014-03-08.

[2]"Insider Threat Blog". CERT. Retrieved 10 August 2012.

[3]"Insider Threat 2018 Report". Cybersecurity Insiders. Retrieved 2018-12-13.

[4]Waters, Matthew D., "Identifying and Preventing Insider Threats" (2016).

[5]Insiders and Insider Threats by Jeffrey Hunker Jeffrey Hunker Associates LLC.

[6]Christian W. Probst, Technical University of Denmark.