SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with ‘A’ Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit V- Cyber Analysis

Topic :Cloud Security and Application Security

Cloud security is the set of control-based security measures and technology protection, designed to protect online stored resources from **leakage, theft**, and **data loss**.

Protection includes data from **cloud infrastructure, applications**, and **threats.**

Security applications uses a software the same as **SaaS (Software as a Service)** model.

manage security in the cloud

- Cloud service providers have many methods to protect the data.
- Firewall is the central part of cloud architecture.
- The firewall protects the network and the perimeter of end-users. It also protects traffic between various apps stored in the cloud.
- Access control protects data by allowing us to set access lists for various assets.
- Data protection methods include Virtual Private Networks (**VPN**), encryption, or masking.

Benefits of Cloud Security System

- Protecting the Business from Dangers
- Protect against internal threats
- Preventing data loss
- Top threats to the system include **Malware, Ransomware**
- Break the Malware and Ransomware attacks
- Malware poses a severe threat to the businesses.

- More than **90%** of malware comes via email. It is often reassuring that employee's download malware without analysingit.

- Malicious software installs itself on the network to steal files or damage the content once it is downloaded.

- **Ransomware** is a malware that hijacks system's data and asks for a financial ransom. Companies are reluctant to give ransom because they want their data back.

- Data redundancy provides the option to pay a ransom for your data. You can get that was stolen with **minimal** service interruption.

- Many cloud data protection solutions identify **malware** and **ransomware**. Firewalls keep malicious email out of the inbox.

DDoS Security

- **Distributed Denial of Service** (DDoS)is flooded with requests.
- Website slows down the downloading until it crashes to handle the number of requests.
- DDoS attacks come with many serious side effects.

Threat to detect

- Cloud computing detects advanced threats by using endpoint scanning for threats at the **device level**.

Difference between Cloud Security and Traditional IT Security

Cloud security	Traditional IT Security
Quick scalable	Slow scaling
Efficient resource utilization	Lower efficiency
Usage-based cost	Higher cost
Third-party data centres	In-house data centres
Reduced time to market	Longer time to market
Low upfront infrastructure	High Upfronts costs

7 Advanced Cloud Security Challenges

- It becomes more challenging when adopting modern cloud approaches Like: **automated cloud integration**, and **continuous deployment (CI/CD)** methods, distributed serverless architecture, and short-term assets for tasks such as a service and container.

- Some of the advanced cloud-native security challenge and many layers of risk faced by today's cloud-oriented organizations are below:

Enlarged Surface

- Public cloud environments have become a large and highly attractive surface for hackers and disrupt workloads and data in the cloud.
- Malware, zero-day, account acquisition and many malicious threats have become day-to-day more dangerous.

Lack of visibility and tracking

- Cloud providers have complete control over the infrastructure layer and cannot expose it to their customers in the **IaaS** model.
- The lack of visibility and control is further enhanced in the **SaaS** cloud models.
- Cloud customers are often unable to identify their cloud assets or visualize their cloud environments effectively.

Ever-changing workload

- Cloud assets are dynamically demoted at scale and velocity.
- Traditional security tools implement protection policies in a flexible and dynamic environment with an ever-changing and short-term workload.

DevOps, DevSecOps and Automation

- Organizations are adopting an automated **DevOps CI/CD** culture that ensures the appropriate security controls are **identified** and **embedded**in the development cycle in code and templates.
- Security-related changes implemented *after* the workload is deployed to production can weaken the organization's security posture and lengthen the time to market.

Granular privileges and critical management

- At the application level, configured keys and privileges expose the session to security risks.
- Often cloud user roles are loosely configured, providing broad privileges beyond the requirement.
- An example is allowing untrained users or users to delete or write databases with no business to delete or add database assets.

Complex environment

- These days the methods and tools work seamlessly on public cloud providers, private cloud providers, and on-premises manage persistent security in hybrid and multi-cloud environments-it including geographic Branch office edge security for formally distributed organizations.

Cloud Compliance and Governance

- All the leading cloud providers have known themselves best, such as **PCI 3.2, NIST 800-53, HIPAA** and **GDPR**.

- It gives the poor visibility and dynamics of cloud environments. The compliance audit process becomes close to mission impossible unless the devices are used to receive compliance checks and issue real-time alerts.\

Application Security

- ***Application security is the process of protecting websites and online services against different security threats that exploit vulnerabilities in an application’s code.***

- Common targets for web application attacks are content management systems (e.g., WordPress), database administration tools (e.g., phpMyAdmin) and Software-as-a-Service(SaaS) applications.
- To become a trusted cybersecurity professional enroll now in the **CISSP Certification** and get certified.

- **Reasons, why web-applications seem to be the most favorite target, are:**
- **Coding practices**
- If the code is poorly written hackers can exploit application-layer loopholes to initiate an attack
- If the code is complex, it increases the likelihood of unattended vulnerabilities and malicious code manipulation

Ease Of Execution

- Most attacks can be easily automated and launched indiscriminately against thousands, or even tens or hundreds of thousands of targets at a time.

- Cybercriminals get paid in bulk amount to attack applications

Application security checklist

‘Prevention is better than cure’. Most of the time organizations have countermeasures to ensure safety against these attacks.

These countermeasures can take the form of software, hardware, and modes of behavior.

Software countermeasures include:

- **Web application firewalls**: Firewalls are usually designed to examine incoming traffic to block attack attempts, thereby compensating for any code manipulation
- **Pop-up blockers**: Also known as pop-up killers prevents pop-ups from displaying in a user’s Web browser
- **Cryptography**: Different kind of encryption and decryption algorithms can be used to secure all the data transmissions
- **Spyware detection programs**: Variety of spyware detection and spyware removal programs can be installed to prevent cyber attacks

Hardware countermeasures include

- A router that can prevent the IP address of an individual computer from being directly visible on the Internet

- Biometric authentication systems that identify third-party hosted content, keeping your application safe

- Intrusion detectors and alarms

Behavioral countermeasures include

- Frequent deletion of stored cookies and temporary files from Web browsers
- Regular installation of updates and patches for operating systems
- Regular scanning for viruses and other malware
- Refraining from opening e-mail messages and attachments from unknown senders

Any Query????

Thank you……