Threats of web and cloud

Science, Computer Science

The role of the security analyst while preventing web server, application and database attacks: 1) in perspective of web server and application: he will monitor the logs and he may also use log monitoring tools . Here he will check what are the ip’s accessing web pages. And also check whether there are any intruders. The main thing he will check about: i)SQL injection ii)brute drive protection iii)malware iv)cross website scripting v)denial of service vi)buffer overflow in perspective of the database : here analyst will check in the following areas i)Excessive previlages ii)database injections iii)malware iv)data loss v)un managed sensitive data these roles may differ in different organizations => some organizations may have as a security analyst, and some of the organization may categorize them according to their requirement. For example, some organization may have security analyst for only web server and applications, and database security analyst => if the organization in dealing big in databases related issues he may categorize them according to this requirement.

So this type of organization requires a database security analyst => if an organization is dealing with application related issues and database too then they need them both. The development of the cloud service model delivers business-supporting technology more efficiently than ever before. Cloud services transforming business and government and created new security challenges. The enterprise authentication and authorization framework do not naturally extend into the cloud. How does a company meld its existing framework to include cloud resources? Furthermore, how does an enterprise merge cloud security data (if even available) with its own security metrics and policies?

One of the most significant barriers to adoption cloud service is security issues regarding compliance, privacy, and legal matters. Providers of cloud services claim that there infra is much secure with advanced up-to-date technology. Here, we have limited control over the cloud infra where your services/applications been deployed. The physical presence of the infra remains secret/unknown so human reachability to devices with an intention to damage can be restricted. Advantages of a system that provides licenses and costs of Internet service:

1. End users want fairness and flexibility and software vendors do not vote for a reduction in revenue. Licensing the distributed cloud servers provides both parties with their own advantages.
2. Software manufacturers need to change the way licensing works and use flexible and non-hardware based licensing solutions that better fit into a virtual environment.
3. Scalability and integration is another good advantage that we can achieve by providing licenses as it is the bilateral agreement which best suits for integration.

Disadvantages of a system that provides licenses and costs of Internet service:

1. Though this approach technically feasible it raises a number of legal issues since many license contracts limit the use of a software license outside a company or outside a certain radius from the company.
2. Running applications protected with this kind of licensing technology developed for centralized computing infrastructures in a distributed service-oriented infrastructure is impossible or at least illegal.

3. When using resources that are spread across different administrative domains, that does not host the application’s license server.

Computer Cloud Failure reasons:

1. Insecure Interfaces and APIs are one of the reasons for cloud server failure as the data flow occurs by these.
2. Failure can also occur through Shared Technology Issues.
3. Data Loss or Leakage happened when the security breach occurs through using a virtual system.
4. Hardware Failure of the central server and appropriate back up is not available.
5. Processes such as inadequate security audits, poor backup procedures, and administrators with inappropriate access to servers are all procedural problems that could be avoided.
6. Closure of Cloud Service: Disputes with the cloud provider or non-profitability of the cloud service may result in the termination of the cloud service, leading to data loss unless end-users are legally protected.
7. Providers cannot cater to sudden spikes in demand, perhaps due to the insufficient provisioning of computing resources and/or poor network design. This happens because of Inadequate Infrastructure Design and Planning