Assignment: Identifying security threats in cloud Human Resource Management System (HRMS) through cloud taxonomy. Name: Anwar Iqbal; Student ID: 18013217

Security threats posed in a cloud environment can be categorized in different ways. Hashemi & Ardakani (2012) presents a taxonomy based on cloud computing service model layers ad administration factor; Gupta & Kumar (2013) presents a taxonomy on the basis of attacks on the service layers. Juliadotter & Choo (2015) presents a taxonomy on the flow of an attack by categorizing dimensions on a cloud service; Ahmed & Litchfield (2016) presents another taxonomy by applying the heuristic approach in identifying cloud threats. Here, the different security threats are analyzed mainly following the taxonomy provided by Ahmed & Litchfield (2016).

In the project migration of HRMS to a cloud HRMS is sought and here possible security threats a cloud HRMS could face are identified. The HRMS will contain employees' personal information and poses a serious challenge related to privacy. The HRMS will also contain modules related to the company's hiring, onboarding and retaining, payroll management, performance management. All of this is sensitive data which if accessed could provide an edge to the competitor's organization. So it is imperative to address the security issues related to a cloud HRMS. The security threats a cloud-based HRMS could face are:

Security threats at user's end:
Confidentiality: There could be attempts to seek personal information related to employees by intercepting the network channel provided by the cloud network (Gupta & Kumar, 2013).
Denial of Service attacks: An attack such as a DDoS attack could prevent employees and HR's to access the requested information (Gupta & Kumar, 2013).

Gaining unauthorized access: Illegal gain of identity by masquerading as a privileged user is an issue posed to cloud HRMS. Eavesdropping on the network and getting passwords that are not encrypted, guessing a weak password or gaining access to the database where all the passwords are stored could enable unauthorized access to the information in the cloud HRM (Gupta & Kumar, 2013). This is an issue which could be analyzed in a social context (Ahmed & Litchfield, 2016).

Access Rights: There are issues related to Authentication and Authorization posed in a cloud environment as the HRMS could be prone to sniffing, phishing or other attacks such as SQL injection, cross-site scripting (Gupta & Kumar, 2013; Ahmed & Litchfield, 2016). Unauthorized access could be obtained by exploiting design weakness or programming vulnerabilities thus causing privilege escalation (Gupta & Kumar, 2013).

Network Security: Domain Name Server (DNS) attack, TCP Hijacking, IP fragmentation attack, session hijacking, network intrusion, eavesdropping, prefix hijacking are some of the attacks that could render the network vulnerable.

Risks associated with virtualization: Virtualization platforms are subject to security risks from external and internal interfaces of cloud (Gupta & Kumar, 2013). Malicious cloud insiders with certain privileges could install keystroke loggers or it could also rest in the hypervisor running beneath the OS. Monitoring Virtual Machines (VM) from the host or from another VM or getting access through VM backdoors, external modification to the hypervisor are some of the ways in which VM vulnerabilities could be exploited (Gupta & Kumar, 2013).

Regulations and Compliance related threats: As we seek to build a cloud HRMS that could offer managing of global employees spanning across different countries and states it poses a challenge related to location transparency, the lack of uniform compliance and regulation related to data handling across different countries or states (Ahmed & Litchfield, 2016).

Exploiting code vulnerabilities: Buffer overflow could be triggered with malicious intent for attacking which could enable a user to alter privileges or to gain unauthorized access. Trojan Horses or Malware also posed serious threats to the cloud (Gupta & Kumar, 2013).

Attacks on Application Layer: Cookie poisoning, Captcha breaking, hidden field manipulation can be used to cause invalid changes in data in a VM's host OS. DDoS is a type of Denial of Service attack which targets the application layer thus rendering some of the cloud resources unusable (Gupta & Kumar, 2013).

SLA provisioning and Trust factor: Possible exploitation of a vulnerability in an SLA by the cloud service provider to absolve themselves from certain responsibilities related to security thus also affecting the trust factor between the provider and the subscriber is another security related concern. (Ahmed & Litchfield, 2016)

References:

Ahmed, M., & Litchfield, A. T. (2018). Taxonomy for identification of security issues in cloud computing environments. *Journal of Computer Information Systems*, *58*(1), 79-88.

Gupta, S., & Kumar, P. (2013). Taxonomy of cloud security. *International journal of computer science, engineering and applications*, *3*(5), 47.

Hashemi, S. M., & Ardakani, M. R. M. (2012). Taxonomy of the security aspects of cloud computing systems-a survey. *networks*, *2*, 1Virtualization.

Juliadotter, N. V., & Choo, K. K. R. (2015). Cloud attack and risk assessment taxonomy. *IEEE Cloud Computing*, *2*(1), 14-20.