Avalon Information Management Security Inc.

Avalon Information Management Security Inc. (AIMS), provides you with the necessary security guidance to assist with identifying your cloud computing security needs to ensure you benefit from your Service Provider offerings in a secure and risk managed approach.

For Security Consulting Services For Cloud Computing, Contact Us at:

(613) 447-9503 (709) 229-6753

The following provides a basic overview of the more prevalent security threats that apply to any IT environment and certainly to cloud computing:

1. *Insider Abuse of Privileges: Some individuals may be coerced by criminals to access client data or facilitate others to gain access to client data. In many situations, these individuals have escalated access privileges and may have access to areas that may not have adequate separation of duties which facilitates this abuse.*
2. *Unauthorized Access: By exploiting weak or improperly secured Application Programming Interfaces (API), an attacker may gain access to system resources and/or sensitive data.*
3. *Exploitation of Multi-tenant Privileges: When a service provider utilizes sharing of resources such as VMware, exploitation of a hypervisor may allow outsiders to gain access to other customers' data and/or services.*
4. *Brute Force Attack: execution of this threat e requires computing power and time, both of which are readily available to most hackers. To facilitate such an attack, an attacker can glean information such as USERID and Password parameters to limit the number of permutations.*
5. *Buffer Overflows. The maximum size of a particular variable is exceeded and submitted to a program for processing. A successful attack will allow an attacker to execute carefully crafted code to gain control of the program and/or backend database.*
6. *Session Hijacking: By using cookie replay attacks, a previously valid cookie resent to a server may allow a prior authenticated session appear valid and continue..*
7. *Cross-site scripting (XSS). An attacker is able to inject executable code into a stream of data within the browser. The code may be executed and allow elevated privileges to sensitive data or programs.*
8. *Denial of Service (DoS) Attack: This type of attack often renders a site, service or application unavailable to authorized users. It can be executed by flooding a server with requests to utilize all available system resource or by transmitting malformed data for input to a server and crashing it or applications on the server..*

NOTICE

The information contained in this document is provided as a simple convenience for the Company's clients and/or prospective clients. The Company has provided the information in good faith and has made reasonable efforts to ensure the information is reasonably accurate and complete. The information made available herein is provided "as is". The Company expressly disclaims all representations and warranties of any kind regarding the contents or use of the information including, but not limited to, express and implied warranties of merchantability, fitness for a particular use, or non-infringement. In no event will the Company be liable for any direct, indirect, special, incidental or consequential damages, including lost profits, lost business or lost data, resulting from the use of or reliance upon the information, whether or not the Company has been advised of the possibility of such damages.

9. *Man-in-the-middle Attacks: A person intercepts both the client and server communications and then acts as an intermediary between the two without each ever knowing. This gives the “middle man” the ability to read and potentially modify messages from either party in order to implement another type of attack listed here.*
10. *Electronic Eavesdropping: This approach allows an attacker to monitor network-based traffgic in an attempt to collect other data that may facilitate access.*
11. *Spoofing Attacks: This is an effort made by an attacker to gain unauthorized access to a system or service by using a false identity acquired by theft or faking a source IP address to facilitate routing to an inner layer. Once successful, an attacker gains access as a legitimate user or host, elevation of privileges or abuse using authorization can begin.*
12. *SQL Injection Attack: This type of attack is facilitated by the failure of an application to validate input in cases where the input is used to construct a SQL statement or will modify the construction of a SQL statement in a particular way. If the attacker can influence the creation of a SQL statement, access to the database with privileges may be possible and, in turn used in to obtain valuable data or modify information or destroy data.*

NOTICE

The information contained in this document is provided as a simple convenience for the Company’s clients and/or prospective clients. The Company has provided the information in good faith and has made reasonable efforts to ensure the information is reasonably accurate and complete. The information made available herein is provided "as is". The Company expressly disclaims all representations and warranties of any kind regarding the contents or use of the information including, but not limited to, express and implied warranties of merchantability, fitness for a particular use, or non-infringement. In no event will the Company be liable for any direct, indirect, special, incidental or consequential damages, including lost profits, lost business or lost data, resulting from the use of or reliance upon the information, whether or not the Company has been advised of the possibility of such damages.

Avalon Information Management Security Inc.

Avalon Information Management Security Inc. (AIMS), provides you with the necessary security guidance to assist with identifying your cloud computing security needs to ensure you benefit from your Service Provider offerings in a secure and risk managed approach.

For Security Consulting Services For Cloud Computing, Contact Us at:

(613) 447-9503 (709) 229-6753

1 Security Considerations

Cloud computing can be a significant cost saver for many IT applications and definitely a business enabler. The common security issues associated with cloud computing are not trivial; however, once understood, customer and SP risk mitigation strategies can be applied to satisfy business objectives. Some of the common security issues include:

- *Security Governance;*
- *Portability (i.e. changing SP);*
- *Multi-tenancy and component failures;*
- *Legal, Regulatory and Customer Policy-specific Compliance;*
- *Customer Management Interface Compromises;*
- *Data Protection (Confidentiality, Integrity and Availability);*
- *Secure Data Retention and Disposal; and*
- *Service Provide Malicious activity (insider access)*

All of these issues can be addressed and security strategies developed, including transferring certain risks to the SP.

Both consumers and Service providers should address the following aspects of security to establish adequate assurances for suitable information protection:

- *Personnel security requirements, including roles, and responsibilities*
- *Regulatory requirements (Privacy Act, PIPEDA*
- *Service availability*
- *Problem reporting, review, and resolution*
- *Information handling and disclosure agreements and procedures (Information sharing)*
- *Physical and logical access controls*
- *Network access control*
- *Data protection (Confidentiality Integrity Availability)*
- *System configuration and patch management*
- *Backup and recovery*
- *Data retention and Disposal (sanitization)*
- *Vulnerability scanning*

NOTICE

The information contained in this document is provided as a simple convenience for the Company's clients and/or prospective clients. The Company has provided the information in good faith and has made reasonable efforts to ensure the information is reasonably accurate and complete. The information made available herein is provided "as is". The Company expressly disclaims all representations and warranties of any kind regarding the contents or use of the information including, but not limited to, express and implied warranties of merchantability, fitness for a particular use, or non-infringement. In no event will the Company be liable for any direct, indirect, special, incidental or consequential damages, including lost profits, lost business or lost data, resulting from the use of or reliance upon the information, whether or not the Company has been advised of the possibility of such damages.

- *Risk management (includes TRA)*
- *Incident reporting, handling, and response*
- *Continuity of operations (BCP)*
- *Resource management*
- *Certification and Accreditation (C&A, ISO27001)*
- *Assurance levels*
- *Independent auditing of services.*

Avalon Security certified professionals can assist with any or all of the security issues and facilitate adequate business objective achievements by working with both customers and Service Providers.

NOTICE

The information contained in this document is provided as a simple convenience for the Company's clients and/or prospective clients. The Company has provided the information in good faith and has made reasonable efforts to ensure the information is reasonably accurate and complete. The information made available herein is provided "as is". The Company expressly disclaims all representations and warranties of any kind regarding the contents or use of the information including, but not limited to, express and implied warranties of merchantability, fitness for a particular use, or non-infringement. In no event will the Company be liable for any direct, indirect, special, incidental or consequential damages, including lost profits, lost business or lost data, resulting from the use of or reliance upon the information, whether or not the Company has been advised of the possibility of such damages.