TRIGENT

Cloud Computing and Security and Privacy

The Trigent Team

Trigent ■ 2 Willow Street, Suite 201, Southborough, MA 01745 ■ 1-877-387-4436 ■ www.trigent.com

Overview

In a recent edition of The New York Times, an article was published with the title of Lost in the Cloud which was primarily about the "real dangers" of cloud computing and the lack of security and privacy. Although the article has some merit relative to the lack of maturity of security and cloud computing broadly, it did not set the context of cloud computing and how to incorporate appropriate security and mitigate against the lack of generic security of cloud computing.

There are three distinct cloud service delivery models: **1.** Software-as-a-Service (SaaS), **2.** Platform-as-a-Service (PaaS) and **3.** Infrastructure-as-a-Service (IaaS). These three models are distinct, at different stages in their maturity lifecycle and have different security ramifications. For example, SaaS is the oldest, most mature, secure and stable model and has been around since 1999. Salesforce.com is the founder of and leader of the SaaS model. PaaS is the next most mature and stable delivery model. One of the "pure play" PaaS providers is OpSource which has been in business since 2002. Many of the PaaS provides such as Rackspace have been around for quite some time and were previously known as ASPs or MSPs. The IaaS delivery model is much more recent and major entrants include Amazon, Microsoft, IBM and Google. Amazon is the most established cloud entrant, however, their Elastic Compute Cloud (EC2) service has only been generally available in the market since 2008.

There are also four cloud service deployment and consumption modes which include: **1.**Public, **2.**Managed, **3.**Private and **4.**Hybrid (i.e., a combination of public and private deployments). The four cloud service deployment and consumption modes should also be considered relative to assessing the "real dangers" of cloud computing and security and mitigation methods.

It is important to understand the advantages, disadvantages, maturity levels and risks of the different cloud service delivery and deployment models in order to leverage best practice solutions for companies and to ensure a stable computing environment with appropriate security. For example, for our clients in general and one of our specific clients, SentryBlue, Trigent and SentryBlue have developed the first comprehensive Critical Incident Management (CIM) SaaS-based solution and deployed it on Northstar Technology Group's public, PaaS platform. SentryBlue adopted best practices of developing a SaaS solution in order to manage customer ease of uses, responsiveness and support, as well as to achieve speed to market, software quality and cost effectiveness. SentryBlue also adopted best practices by running its SaaS solution on a proven, stable and secure third-party PaaS platform (Northstar) and leveraging an independent offshore software development and support partner (Trigent).

Representative security considerations, best practices and layers for the SentryBlue solution are broken down, focused and implemented as follows:

SentryBlue SaaS Service

- One way encrypted passwords used for user authorization/authentication
- Secure Sockets Layer (SSL) – Digital certificate authority enabling secure e-commerce communications and interacting with web sites and intranets
- Information protection from unauthorized discovery over the network
- Ensuring that the data provided is secure and the employees of the SaaS provider are not in a position to misuse the data
- Payment Card Industry (PCI) Data Security Standard (DSS) for billing and payment processing
- Rapid bug fixes, enhancements and iterative releases go through extensive testing and are only published by trusted sources
- Data portability and separation from the application and PaaS platform

Northstar Facility and Monitoring

- Internal and external 24/7 security monitoring
- Ensuring valid identity and connected device security and compliance
- Multiple ISP connections and dual fiber entrances for redundancy
- Card key access system
- Power distribution monitoring and dual power feed
- Redundant generator backup
- Temperature and water monitoring
- Fire detection and suppression system
- Concrete enclosed facility rated to withstand an F3 Tornado

Northstar PaaS Service

- Offsite/off-premise for both private and special needs schools and SentryBlue for critical incident management and recovery
- Intrusion Detection Software (IDS) for firewall rule sets
- 1024 bit encryption to secure communication from the Web browser to the host computer
- Valid identity and connected device security policy compliance
- Frequent application of server hardening techniques including bug fixes, security patches, penetration testing, etc. to ensure that the underlying systems (i.e., Web, database, application servers) are secure
- Performance of both internal and external penetration testing
- Data security and privacy behind Northstar's firewall
- High availability and recovery
- Disaster recovery and business continuity planning – Addressing what happens in the event of a disaster and how quickly the application can be up and running in the event of a disaster

Regulatory and Compliance

- Third-party SAS 70 security and privacy audit compliance
- Payment Card Industry (PCI) Data Security Standard (DSS) for billing and payment processing

Summary

Segments of cloud computing (i.e., SaaS, PaaS and the physical facility) are being secured and protected today. Moreover, the security best practices are typically superior than those provided by most small and mid-size organizations because of their limited technical resources and budget constraints. The cost, return and extensiveness of the aforementioned security best practices are spread across multiple customers and would be a challenge to be afforded or deployed by an individual small and mid-size organization on a stand-alone basis.

About Trigent Software Inc.

Trigent is a privately held, professional IT services company and a Microsoft Gold Partner with its U.S. headquarters in the greater Boston area and its Indian headquarters in Bangalore. We provide consulting services in various technologies including Microsoft Solutions. Our operating model is to conduct sales, customer relationships and front-end consulting (e.g., business case, requirements, architecture) onsite with our clients and perform the detail design, development, integration, testing and quality assurance offshore at our world class development and support center in Bangalore. We are a SEI CMM Level 4 company and is ISO 9001:2000 TickIT certified organization.

For sales contact sales@trigent.com or call 508-490-6000.

Microsoft Partner
Gold Application Development
Gold Collaboration and Content
Silver Mobility