Microsoft

Effective Practices for Cloud Security

Effective Security Practices Series

Moving some internal processes to the cloud initially looks appealing: lower capital costs, more centralized management and control, and the ability to leverage shared resources and expertise. Groups like the Cloud Security Alliance have identified key security challenges and their work has shown that businesses need to tread carefully. In this paper we look at some effective practices around cloud computing and security. What are some of the key challenges that enterprises are facing around cloud security? How are enterprises managing security in cloud migrations today? How are businesses crafting Service Level Agreements (SLAs) with cloud providers? How are enterprises reconciling cloud-based deployments with the rigors of audit? While the cloud is not new, there is a surge of options to move some operational aspects of the business externally. This paper looks at how enterprises are managing these opportunities and the associated security challenges.

Herbert H. Thompson, Ph.D.
Chief Security Strategist, People Security

The information contained in this document represents the current view of Microsoft Corp. on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Preface

Information security is a very dynamic field: legislation keeps changing, technology keeps evolving, and the attacker community continues to become more sophisticated. This turmoil has forced security practitioners to think creatively to address some very difficult problems. Much of this innovation has been locked away within corporations as they have made isolated progress on issues like security metrics, security risk management frameworks, and security policy. In order to address this discrepancy, Microsoft commissioned a whitepaper series to share key security innovations. Whitepaper topics came from participants in Microsoft's CSO Council - a semi-annual gathering of security executives from leading global organizations who serve as advisors to Microsoft's Trustworthy Computing Group.

Our goal is to share practices "from-the-trenches" that address some of the toughest problems in security. After numerous interviews, discussions, and debates with these though leaders, a collection of effective practices emerged. While much remains to be done, we hope that these whitepapers fuel the discussion and help facilitate further sharing in the field of IT security.

Overview

Service Oriented Architecture (SOA), Software as a Service (SaaS), and other computing models now come largely under the umbrella of Cloud Computing. While the concept of cloud computing is not new, the availability of solutions, coupled with economic pressures to cut expenses, has motivated many companies to take a serious look at migrating some IT services to the cloud. This paper looks at some of the key challenges of cloud security from the perspective of enterprise CISOs. It also presents practices for managing cloud security that have been effectively applied by enterprises.

The information provided here is based on numerous discussions and interviews with security architects and security executives in large enterprises. While it does not address the breadth of cloud security issues, it outlines some of the current attitudes and approaches of interviewees. Many vendors and industry groups are working on cloud security and have made some progress in defining fundamental challenges and solutions. Groups such as the Cloud Security Alliance (CSA)[1], the European Network and Information Security Agency (ENISA)[2], and others have done significant work in defining a large set of security challenges corporations need to consider while moving to the cloud. This document, by contrast, looks at how several large enterprises have dealt with some of the security challenges of the cloud in practice.

The Case for Cloud

At initial review, the case for moving some services to the cloud is compelling. Cloud computing promises a use-based model, one where resources are paid for as they are consumed. Instead of front-loading project cost, expenses can be amortized over the life of the system as Operational Expenditure (OpEx). This has the added benefit of agility; businesses may be able to better adapt to changes in needs and provision new systems and configurations quickly. Additionally, moving some operations to the cloud can push off problematic issues of maintenance and upkeep to the cloud service provider.

Some cloud providers can justify bringing specialized skills in-house and this cost is spread among clients. Cloud providers also offer elastic expansion of computing power or bandwidth as needed with a consumption-based cost model. This is compelling when

[1] www.cloudsecurityalliance.org

[2] http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

handling occasional spikes in load. Additionally, having the ability to replicate data across multiple servers in multiple physical locations supports data redundancy and availability.

Cloud computing also has the potential to improve security for some deployment cases. Pooled resources can allow cloud service providers to weave security into the fabric of their infrastructure and software. Additionally, centralized management of resources can allow enterprises to more easily implement configuration changes. Despite the many benefits of cloud computing, there are important issues of corporate governance that are largely unresolved.

Cloud Meets Security

In writing this paper we talked with several Chief Information Security Offices (CISOs) and security architects in large enterprises about the security challenges they faced in moving some operational aspects of their business to the cloud. The concerns, ideas, and practices expressed here were based on a sampling of large enterprises as opposed to small and medium sized businesses (SMBs). While many of these issues also impact SMBs, the focus is on enterprise deployments.

Most enterprises that we talked to had already made some foray into the cloud, primarily in areas that did not involve legally protected data or personally identifiable information (PII). Universally, respondents expressed their company's interest in exploring the cloud as a deployment option. The most commonly cited roadblock was audit. Respondents were most concerned about being able to get answers to answer basic audit questions from cloud providers about who was managing their data, where the data was physically located, and in many cases, the nationality of administrators who may have access to their data. The following summarizes the most common concerns and practices on key cloud issues:

Audit

Concern over audit was one of the most commonly cited issues. Many respondents felt they were given insufficient information or guarantees by some cloud providers on how their information was handled internally. They found it difficult to get answers to some basic questions such as: What security controls are in place to protect our data? Where is our data physically located (primarily concerned about country)? Who has access to the data? What is the nationality of people who have access to our data? Many expressed the need to inspect and monitor the cloud provider's facilities either directly or through some independent 3rd party. For any deployment involving legally protected data respondents only considered providers that could give them clear answers to key audit questions. Further, they required that answers to these questions be explicit incorporated into Service Level Agreements.

Security controls and protection

Respondents needed assurance about the security controls that were put in place by the cloud service provider. For Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) deployments, respondents wanted information about network topology and security practices that could then be clearly communicated to audit and enterprise risk management groups. For SaaS deployments, participants discussed the need for documented secure coding practices and – depending on the sensitivity of the data managed – possible security (penetration) testing results from 3rd parties. While many believed software security to be important, few had any contractual language that explicitly addressed software security (although they planned on incorporating such language in the future). Specific requirements for other security controls were largely audit-driven.

Managing the increased risk of pooled data (attack and e-discovery)

A significant concern was that the enterprise might be collaterally damaged during some incident involving another tenant of the cloud service provider. These concerns fell into two groups. The first was concern that they might be at increased risk of attack depending on the other customers that shared their resources. An analogous example was the politically motivated denial of service attacks against a single Twitter user that caused outages for all users. They also expressed concerns that the aggregation of data from multiple companies in one spot poses a very attractive target for attackers who may be willing to expend significant resources during attack. The result could be to put each individual cloud tenant at increased risk. A second set of concerns revolved around e-discovery and legal action that might be taken against another tenant. For this reason, many respondents required assurance of isolation for deployment scenarios involving highly sensitive data.

Transparency

Depending on the deployment model, a significant amount of information about the operational aspects of a cloud service provider may be abstracted from customers. There were some concerns raised about transparency and the need for operational-level information to be available for review both by enterprise security personnel and by internal/external auditors. Responses varied significantly in this area. While transparency was expressed as a key concern, many respondents relied on the terms of SLAs as opposed to actual facility audits.

Lack of benchmarks and evaluation standards

Several respondents expressed concerns over a lack of standard evaluation criteria for cloud service providers. This was a particular challenge when communicating potential risk to internal and external auditors. Some respondents pointed to the European Network and Information Security Agency's (ENISA's)[3] release of a set of evaluation criteria for cloud service providers as a potential baseline for future cloud provider assessments.

Update and System Changes

Specific to SaaS there was some concern among respondents around updates to applications and the potential impact that could have. Concerns fell into two groups. The first was potential instability resulting from a system change. Some SaaS providers were on regular update schedules which helped to mitigate concerns. Additionally, some SaaS providers had a written policy of providing advanced notice of any updates or patches at the software level. Few SaaS providers communicated information about OS-level patches and updates. The second concern was around changes to application interfaces. and they stressed the need for consistency. This was a significant concern for companies that interfaced programmatically with SaaS providers. These concerns were primarily addressed by SaaS providers through a communicated set of policies around the timing and interface impact of system updates.

Service Level Agreements (SLAs)

There were several open issues reported with crafting cloud service provider SLAs. Feedback indicated a severe need for SLA templates and contractual language that enterprises could work from and adapt. There were three areas of particular concern. The first was mapping regulatory and standards requirements to specific terms that fit into an SLA. The second was being able to craft an SLA that cloud providers would accept that still met the burden of internal and external audit. The third was the need for better

[3] http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

processes to map the terms of service in the agreements that enterprises had with their customers to an SLA with cloud providers. Respondents indicated that there was a significant gap, in some cases, between their requirements and the terms that cloud service providers would agree to. Many had to shop around before finding a provider that met their requirements. In all cases, the inability of a cloud provider to meet explicit regulatory requirements would derail a deal. Beyond explicit regulatory requirements, many respondents indicated that security requirements were not adequately detailed in many current provider SLAs.

Open Questions

In addition to the issues above, respondents were asked to list questions they would ideally want answered by cloud service providers. A list of these questions is provided below:

- Can we specify who shares physical (or logical) resources with us?
- What is the defense-in-depth architecture of the system?
- What ability do we have to conduct audits or assessments?
- Will a 3rd party be allowed to audit the system and can we have the results of that audit?
- What are the legal implications of us shifting services/operations to the cloud (e-discovery, etc.)?
- What about e-discovery? Are we covered? Can our data be subpoenaed in a case involving another customer of yours that shares data with us?
- Do we have exposure of being locked out due to legal action taken against another one of your customers?
- Can you provide assurance of data destruction?
- What is the financial viability of the provider and what happens if the provider fails?
- Who is managing our data?
- Where is our data replicated?
- Is our cloud provider SLA in conflict with any of our customer SLAs (right to audit, etc.)?
- For Software-as-a-Service, how can we gain confidence in the security quality of the software?
- What dependencies do our cloud providers have?

- What about a denial of service that comes from a peak load of one of your other customers?

These questions indicate a wide range of concerns that still need to be addressed.

Conclusion

Spurred by a strong business case and the increased availability of deployment options, enterprises are looking for opportunities to move to cloud-based deployments. Some enterprises have held back on cloud migrations for critical or sensitive functions: with concerns about security, governance, and audit being some of the biggest obstacles. Others have moved forward and have had to face these issues directly. More information sharing among practitioners is needed along with practical models for evaluating and safely contracting with cloud providers. This paper presented a collection of concerns and practices for cloud security from information security executives and practitioners in large enterprises. For some deployment scenarios, it is evident that the availability of cloud-based solutions has outpaced supporting security models. The goal of this paper is to encourage further information sharing on cloud security. While the industry has made some significant steps forward, much work remains to be done.