White paper

risk analysis

framework for a cloud specific environment

Turning the key to sound business decisions

Your business technologists. **Powering progress**

Contents

Abstract

Security and compliance are the most intensively discussed topics in the evolving Software as a Service (SaaS) and Cloud Computing market for corporate customers. As with any new technology, new risks evolve from Cloud Computing, some of them potentially capable of jeopardizing the future of a whole company.

Surveys show that security and privacy are seen as blocking points for adoption of Cloud technology, but the discussion about them is often biased. While it is surely right to take a cautious approach to a technology as revolutionary for IT operations as Cloud Computing, it must be remembered that it also offers great new opportunities – especially for the small and medium business sector – and these are often understated.

To take the hysteria out of the debate, a well-founded approach towards assessing the risks associated with Cloud Computing is needed. A first valuable step has been taken by a report from the European Network and Information Security Agency (ENISA), which examines the range of risks associated with Cloud Computing security [1] in general.

This white paper is presented by Atos to help organizations move towards a Cloud specific risk assessment.

Assessing the risk

Simple but challenging answers

How should the risk associated with a specific Cloud service be assessed? The answer is as simple as it is challenging: like any other security-related business decision, the basis for assessment has to be a solid quantification of the associated business risk versus the economic effort that it would take to mitigate or avoid this risk (Figure 1). The economic effort has to include opportunity cost – for example, not realizing a potential saving or business improvement – to reflect the complete dimension of the decision.

How to determine risk

There are many risk assessment methodologies, but they all require similar steps to be carried out. Figure 2 shows the steps used in the National Institute of Standards in Technology (NIST) risk assessment methodology, described in its SP800-30 NIST SP 800-30: Risk Management Guide for Information Technology Systems [2].

The International Organization for Standardization ISO 27005 [7] defines risk as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization", and adds that it is measured in terms of a combination of the likelihood of an event and its consequences. A useful overview of factors contributing to risk as described by The Open Group's risk taxonomy [4] is presented in Figure 3.

The taxonomy exhibits the same two top-level factors of risk also mentioned by ISO 27005 [7]: likelihood of a harmful event (here expressed as "loss event frequency") and its consequences ("probable loss magnitude"). The subfactors of the probable loss magnitude on the right-hand side are an enumeration of the factors influencing the ultimate cost of a harmful event.

The subfactors of the loss event frequency shown on the left-hand side can be explained. A loss event occurs when a threat agent (e.g. a hacker) successfully exploits a vulnerability. The frequency with which this happens depends on:

- The frequency with which threat agents try to exploit a vulnerability. This frequency is determined by the threat agent's motivation to carry out an attack action ("What can he gain with an attack?", "How much effort does it take?", "What is the risk for him?", etc.) and the degree of access ("contact") that the threat agent has to the attack target
- The difference between the threat agent's attack capabilities and the strength of the system to resist the attack. The Open Group's risk taxonomy defines vulnerability as: "the probability that an asset will be unable to resist the actions of a threat agent. Vulnerability exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force."

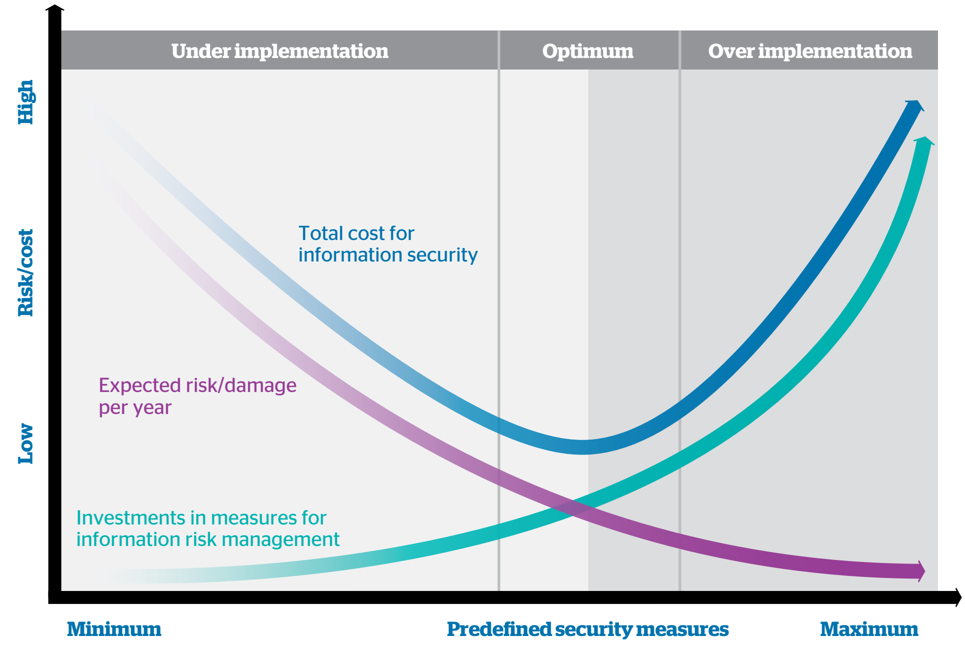
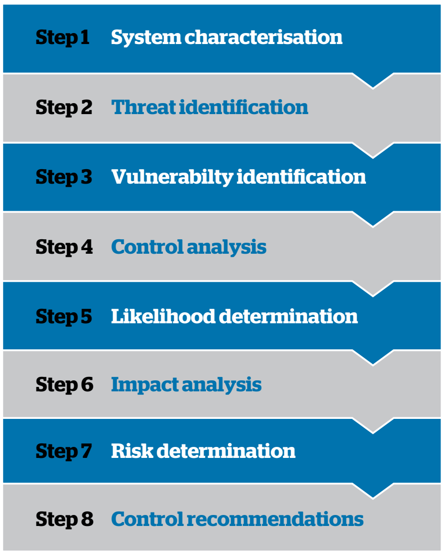


Figure 1: risk/cost optimization using information risk management.



Step 1 System characterisation

Step 2 Threat identification

Step 3 Vulnerabilty identification

Step 4 Control analysis

Step 5 Likelihood determination

Step 6 Impact analysis

Step 7 Risk determination

Step 8 Control recommendations

Figure 2: Assessment activities according to NIST SP800-30.

Risk assessment is carried out by determining the top-level factors of probable loss frequency and magnitude, based on an examination of these low-level factors that constitute the top-level factors.

Returning to the steps of NIST's assessment methodology as displayed in Figure 2, we see that Steps 2-5 deal with an assessment of loss event frequency, Step 6 examines the probable loss magnitude, and Step 7 combines this information into a risk determination. Step 8 then recommends controls that reduce risk to an acceptable level.

For supporting a Cloud specific risk assessment, we have to examine which risk factors are changed by using a Cloud Computing infrastructure rather than a traditional infrastructure.

From a Cloud customer perspective, the probable magnitude of future loss (right-hand side of the risk factor tree of Figure 3) is not changed at all by Cloud Computing: the consequences and – ultimately – cost of, for example, a breach of confidentiality, is exactly the same regardless of whether the data breach occurred within a Cloud infrastructure or a conventional IT infrastructure.

For a Cloud service provider, things look somewhat different. Because Cloud Computing pools systems on the same infrastructure that were previously separated, a loss event may entail a considerably larger impact. This fact is easily grasped and incorporated into a risk assessment: no conceptual work for adapting impact analysis to Cloud Computing seems necessary.

Cloud specific modifications of the risk assessment approach must therefore apply to the left-hand side of the risk factor tree of Figure 3, the loss event frequency.

Cloud Computing may change the probability of a harmful event occurring. The most drastic changes, if there are any, must concern the factor "vulnerability": moving to a Cloud infrastructure may change the level of access for an attacker as well as the effort and risk associated with an attack action. So these factors must be considered, but for supporting a Cloud specific risk assessment, it seems most profitable to define and examine Cloud specific vulnerabilities.

A prerequisite for understanding this is a comprehensive definition of Cloud Computing: only then is it possible to pinpoint which vulnerabilities are Cloud specific.

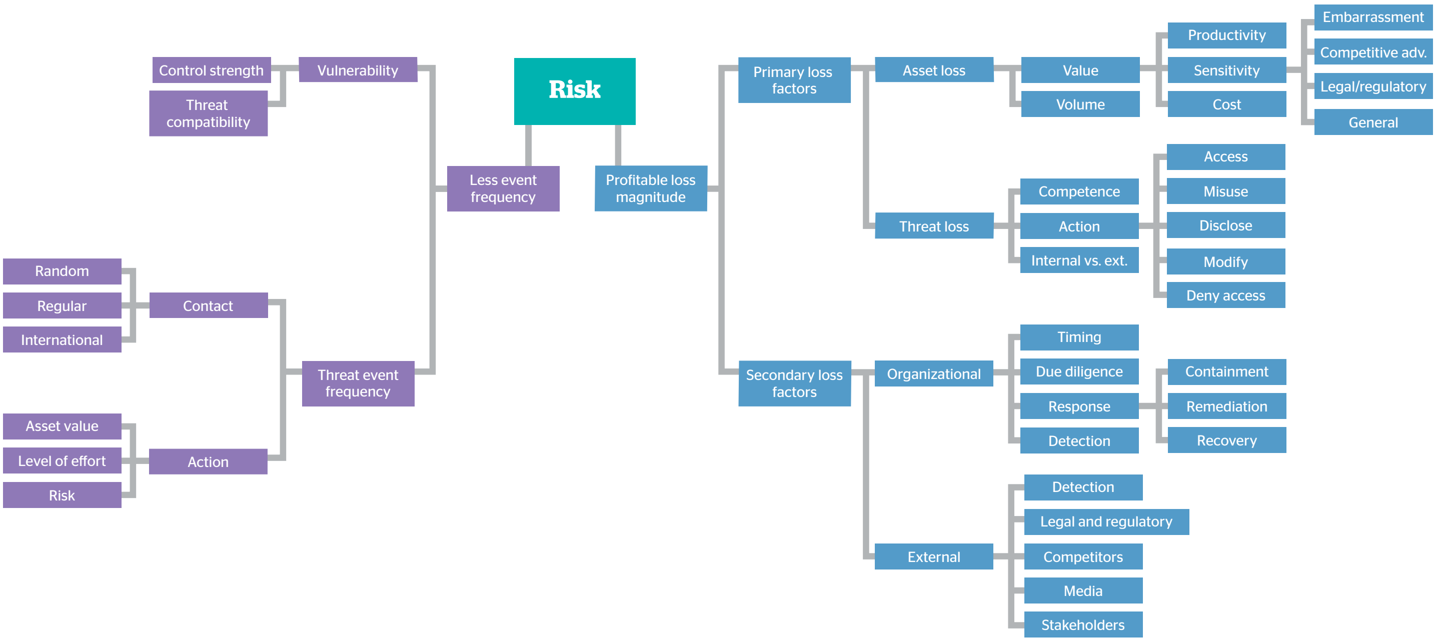


Figure 3: Factors contributing to risk according to The Open Group's risk taxonomy.

An abstract view of Cloud Computing

NIST defines Cloud Computing as follows [9]: Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. A deeper understanding of Cloud Computing can be reached by examining (1) essential characteristics of Cloud Computing, (2) a Cloud Computing reference architecture, and (3) core technologies of Cloud Computing.

Essential characteristics of Cloud Computing

NIST [9] identifies the following essential Cloud characteristics:

On-demand self-service

Users can order and manage services without human interaction with the service provider, using, for example, a web portal and management interface. Provisioning and de-provisioning of services and associated resources occur automatically at the provider.

Ubiquitous network access

Cloud services are accessed via the network, usually the Internet, using standard mechanisms and protocols.

Resource pooling

Computing resources used to provide the Cloud service are realized using a homogeneous infrastructure which is shared between all users of the service.

Rapid elasticity

Resources can be scaled up and down rapidly and elastically.

Measured service

Resource/service usage is constantly metered, supporting optimization of resource usage, usage reporting to the customer and pay-as-you-go business models.

A reference architecture of Cloud Computing

The stack of Cloud service models for Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) is well established. Several extensions/refinements of this stack towards an "ontology" or "reference architecture" have been proposed (e.g., work carried out at UCLA and IBM [6] or by the Cloud Security Alliance [8]). Atos has designed a reference architecture with a special focus on (1) making the most important security-relevant Cloud components explicit, and (2) providing an abstract yet complete overview of Cloud Computing as the basis for the analysis of security issues.

The reference architecture shown in Figure 4 is based on the work carried out at UCLA and IBM [6]. It inherits the layered approach, where layers may encompass one or more service components. Here, "service" must be understood in the broad sense of providing something that may be both material (such as shelter, power, hardware, etc.) as well as immaterial (such as a runtime environment). For two layers, namely "Cloud Software Environment" and "Cloud Software Infrastructure", the model makes the three main service components of these layers – computation, storage and communication – explicit.

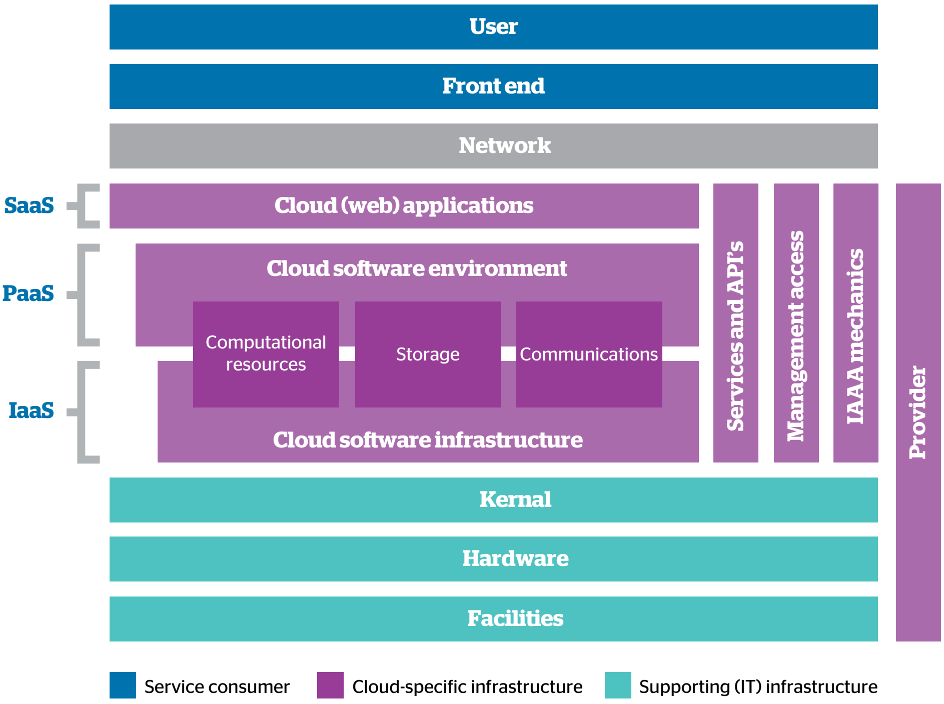


Figure 4: NIST Cloud Reference Architecture

It is important to note that the services in the top layer can be implemented on the basis of layers further down the stack as well, in effect skipping intermediate layers. For example, a Cloud web application can still be implemented and operated in the "traditional" way, namely running on top of a standard operating system without making use of dedicated Cloud software infrastructure and environment components.

Note that layering and compositionality imply that the transition from providing some service/function in-house versus sourcing the service/function can take place between any of the layers exhibited in the model.

In addition to the original model, supporting functions that have relevance for services in several layers have been identified and added to the model as vertical spans over several horizontal layers.

Our Cloud Reference Architecture (see Figure 4) exhibits three main parts:

Supporting (IT) infrastructure

These are facilities/services that are common to any IT service, whether or not they are a Cloud offering. We include them in the reference architecture, because we want to provide the complete picture: a complete treatment of IT security must also take non-Cloud specific components of a Cloud service into account.

Cloud specific infrastructure

These are the infrastructure components that are indeed Cloud specific: Cloud specific vulnerabilities and corresponding controls will be mapped mostly to these components.

Cloud service consumer

In order to provide a complete picture, the Cloud-service customer is included in the reference architecture, as it is of relevance for an all-encompassing security treatment.

The network that separates the Cloud service consumer from the Cloud infrastructure is also made explicit: the fact that access to Cloud resources is carried out via a (usually untrusted) network is one of the main characteristics of Cloud Computing. A detailed description of the service layers and supporting functions contained in the reference architecture is featured overleaf.

Reference model components: service layers

Facilities

Ultimately, any type of service must be physically housed somewhere; in the case of computational services, the underlying hardware must be housed and provided with power, cooling, and network access. "Facilities as a Service" such as the act of renting server space at a data center are commonplace. However, "Facilities as a Service" cannot really be viewed as a Cloud service because service delivery has at its heart a physical component that cannot be carried out via the Internet: somebody has to drive the server to the data center and have it installed there.

Hardware

All Cloud services run on top of physical hardware such as servers and the network components connecting the servers with each other and outside networks. Also "hardware as a service" (HaaS) is as commonplace as non-Cloud service: hardware is rented using traditional methods of closing a contract and service delivery.

However, there may be room for HaaS as a Cloud service in cases where special requirements make virtualization-based IaaS offerings undesirable or impossible. Cloud HaaS would mean that for example servers can be rented and managed with the same methods known from IaaS services such as Amazon EC2. It should be noted, however, that HaaS providers have to address a number of technical challenges in operating and managing their services [6].

Kernel (OS/Apps)

Hardware by itself is useless without a kernel that enables the operation of software on the hardware. The most common instance of such a kernel is an operating system running directly on top of a given piece of hardware.

Recent developments in virtualization technology have introduced the concept of a hypervisor, a kernel that basically provides API access to hardware that is utilized by one or more operating systems running on top of the hypervisor.

When a hypervisor is used, usually one of the operating systems that run on top of it has special rights over the hypervisor, and is used for managing the hypervisor infrastructure. Again, the provisioning of servers with installed (and managed) operating systems as a service is well-established but is unusual as a Cloud service for operating systems running directly on physical servers rather than in a virtualized environment.

An operating system without an application running on the OS is rather useless: we therefore include "applications" in this layer. Thus, the "kernel" layer is the top layer of the supporting IT infrastructure. At least one of the higher layers of the Cloud infrastructure must be implemented directly as an application running within this layer. Depending on which of the higher layers is present in a given Cloud Computing stack, this may be an application realizing a virtualization environment, providing a runtime environment for web services and applications, implementing a web service, etc.

Cloud software infrastructure

The Cloud software infrastructure layer provides a level of abstraction for basic IT resources that are offered as services to higher layers: computational resources (usually in the form of virtual machine environments), storage, and (network) communication. These services can be used individually, as is most often the case with storage services, but are often bundled so that servers are delivered with certain network connectivity and – often – access to storage. This bundle (with or without storage) is usually referred to as IaaS. While the "computational resources" service component of IaaS is already well developed, it seems that "communications as a service" is only now becoming more sophisticated.

Cloud software environment

While the "Cloud software infrastructure" layer provides services on the operating system level, the "Cloud software environment" layer provides services at the level of an application platform: (1) a development and runtime environment for services/applications written in one or more supported languages, (2) storage services (more as database interface rather than file share) and (3) communication infrastructure such as Microsoft Azure's service bus.

Cloud web applications

A web application uses browser technology as a front end for user interaction.

With the increased take-up of technologies for browser-based computing such as Javascript, Java, Flash and Silverlight, a web Cloud application falls into two parts: (1) an application component operated somewhere in the Cloud and (2) a browser component running within the user's browser. Technologies such as Google Gears will increasingly be used in the future to allow offline usage of a web application's browser component for cases in which constant access to remote data is not required.

Service consumer and network

Network

One of the essential characteristics of Cloud services is that they are accessed via the network – usually the internet. In most cases, the network is untrusted, i.e. the presence of attackers who may try to attack the Cloud infrastructure or communication between the Cloud customer and the Cloud infrastructure must be assumed.

Front end

As mentioned on page 9, web Cloud applications fall into two parts, one of which is running on the user's client, usually within the web browser and its plug-ins. The technologies and vulnerabilities of these front end components are therefore relevant for Cloud service technologies and the risks associated with them.

User

It is well known that security cannot succeed without taking the user into account. The Cloud customer is therefore included in the reference architecture as the basis for an all-encompassing security treatment.

Reference model components: supporting functions

Services and APIs

All layers of the Cloud infrastructure offer services, but for examining Cloud infrastructure security, it is worth thinking specifically about all service and application programming interfaces that are present in the infrastructure. Most services are likely to consist of web services (which share many vulnerabilities with web applications) – indeed, the above-mentioned web application layer may be realized completely by one or more web services so that the application URL would only serve for provisioning the user with a browser component. Apart from web services, there may also be service interfaces and APIs of a different nature.

Management access

As NIST's definition of Cloud Computing states: one of the central characteristics of Cloud services is that they can be rapidly provisioned and released with minimal management effort or service provider interaction. Consequently, a common element of each Cloud service is a management interface which in most cases takes the form of a web application. Increasingly, web service based APIs are also offered.

Identity, authentication, authorization and auditing mechanisms

All Cloud services, and the management interface for each, require mechanisms for identity management, authentication, authorization, and auditing (IAAA). To a certain extent, parts of these mechanisms may be factored out as a stand-alone IAA service to be used by other services. Two elements of IAAA that cannot be factored out and must be part of each service implementation are the execution of adequate authorization checks (which, of course, make use of authentication and/or authorization information received from an IAA service) and auditing of the Cloud infrastructure.

Provider

The service provider of a Cloud Computing service can be seen as a supporting function spanning the whole Cloud Computing stack. We include the provider in the model so as to define a location for issues that specifically concern the fact that a service is outsourced.

Core technologies of Cloud Computing

Certain technologies must be considered as core technologies of Cloud Computing, in the sense that Cloud Computing builds heavily on the capabilities available through these technologies.

Currently, we consider the following technologies as Cloud core technologies:

- **Web Applications and Services** SaaS and PaaS is unthinkable without web application and web services technologies: SaaS offerings are typically implemented as web applications, and PaaS offerings provide development and run-time environments for web applications and web services. Also for IaaS offerings, associated services and APIs such as management access for customers are typically implemented using web application / service technologies.
- **Virtualization** IaaS offerings have virtualization techniques at their very heart. Because PaaS and SaaS services are usually built on top of a supporting IaaS infrastructure, the importance of virtualization also extends to these service models. In the future, we expect the resources offered by virtualization to develop from virtualized servers towards computational resources that can be used more readily for executing SaaS services.
- **Cryptography** Many security requirements for Cloud Computing can only be solved using cryptographic techniques. Cryptography therefore must be considered a core technology of Cloud Computing.

Cloud specific vulnerabilities

Based on the abstract view of Cloud Computing presented in the previous section, we can move now towards a definition of what constitutes a Cloud specific vulnerability.

A vulnerability is Cloud specific, if at least one of the following indicators is true. It:

- **Is intrinsic to or prevalent in a core technology of Cloud Computing**
- **Has its root cause in one of NIST's essential Cloud characteristics**
- **Is caused by Cloud innovations making tried and tested security controls hard or impossible to implement**
- **Is prevalent in established state-of-the-art Cloud offerings.**

In the following section, we examine each of these four indicators.

Vulnerabilities intrinsic to core technology of Cloud Computing

The core technologies of Cloud Computing – web applications/services, virtualization, and cryptography – have vulnerabilities that are either intrinsic to the technology or prevalent in state-of-the-art implementations of the technology.

These are a few examples of vulnerabilities:

Virtual machine escape vulnerability

The possibility that an attacker may succeed in escaping from a virtualized environment lies in the very nature of virtualization. Hence, this vulnerability must be considered as intrinsic to virtualization and is obviously highly relevant to Cloud Computing.

Session riding and session hijacking

Web application technologies have to overcome the problem that the HTTP protocol by design is a state-less protocol, whereas web applications require some notion of session state. There are many techniques to implement session handling and – as any security professional knowledgeable in web application security will testify – many implementations of session handling are vulnerable to session riding and session hijacking.

One can argue whether session riding/hijacking vulnerabilities are intrinsic to web application technologies or "only" prevalent in many current implementations. In any case, these vulnerabilities are certainly relevant for Cloud Computing.

Insecure/obsolete cryptography

For all cryptographic mechanisms and algorithms there is the danger that advances in cryptoanalysis may render them insecure by attackers finding novel methods of breaking the cryptography. It is even more common to find crucial flaws in the implementation of cryptographic algorithms that turn a very strong encryption into a very weak encryption (or sometimes no encryption at all).

Because broad take-up of Cloud Computing is unthinkable without the use of cryptography to protect confidentiality and integrity of data in the Cloud, vulnerabilities concerning insecure and/or obsolete cryptography are highly relevant for Cloud Computing.

Vulnerabilities with root cause in an essential Cloud characteristic

As described above, the essential Cloud characteristics according to NIST are:

- On-demand self-service
- Ubiquitous network access
- Resource pooling
- Rapid elasticity
- Measured service.

There are vulnerabilities that can be said to have their root cause in one or more of these characteristics. Here are examples:

Unauthorized access to management interface

The Cloud characteristic "on-demand self-service" requires a management interface that is accessible to users of the Cloud service. Unauthorized access to the management interface therefore is a vulnerability that must be considered especially relevant for Cloud systems. The probability that unauthorized access could occur is much higher than for traditional systems where the management functionality is accessible only to a few administrators.

Intranet protocol vulnerabilities

The Cloud characteristic "ubiquitous network access" states that Cloud services are accessed via the network using standard protocols. In most cases, this network is the Intranet and thus must be considered as an untrusted network. Intranet protocol vulnerabilities, e.g., vulnerabilities that allow man-in-the-middle attacks, are relevant for Cloud Computing.

Data recovery

The Cloud characteristics "pooling" and "elasticity" lead to a situation where resources that have been allocated to one user may be re-allocated to a different user at a later point of time. In the case of memory or storage resources, it may therefore be possible to recover data written by a previous user – hence a vulnerability that has its root cause in the Cloud characteristics.

Metering/billing evasion

According to the Cloud characteristic "measured service", any Cloud service has a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, active user accounts, etc.); and metering data is used for optimization of service delivery as well as billing. Vulnerabilities regarding the manipulation of metering/billing data or billing evasion therefore have their root cause in this particular characteristic of Cloud Computing.

Vulnerabilities caused by defects of known security controls in a Cloud setting

As discussed above, a vulnerability exists when a threat agent's attack capabilities exceed the strength of the system to resist the attack. Hence, the weakness or absence of security control, i.e. a counter measure against certain attacks, constitutes a vulnerability. Vulnerabilities concerning problems with standard security controls must be considered Cloud specific, if Cloud innovations directly cause difficulties in implementing these controls.

We refer to such vulnerabilities as "control challenges". Here are some examples of control challenges:

Insufficient network-based controls in virtualized networks

By the very nature of Cloud services, the administrative access to IaaS network infrastructure and the possibility of tailoring network infrastructure are usually limited: hence, standard controls such as IP-based network zoning usually cannot be applied.

Standard techniques such as network-based vulnerability scanning are usually forbidden by IaaS providers, for example, because "friendly" scans cannot be distinguished from attacker activity.

Finally, technologies such as virtualization lead to a situation where network traffic occurs not only on physical networks but also within virtualized networks (e.g. for communication between two virtual machine environments hosted on the same server). All in all, this constitutes a control challenge, because tried and tested security controls at network level may not work in a given Cloud environment.

Poor key management procedures

As pointed out in a recent study by ENISA [1], Cloud Computing infrastructures require the management and storage of many different kinds of keys. Because virtual machines do not have a fixed hardware infrastructure and Cloud based content tends to be geographically distributed, it is more difficult to apply standard controls, such as hardware security module (HSM) storage, to keys on Cloud infrastructures.

Security metrics not adapted to Cloud infrastructures

Currently, no standardized Cloud specific security metrics exist that could be used by Cloud customers to monitor the security status of their Cloud resources. Until such standard security metrics are developed and implemented, controls with respect to security assessment and the audit and accountability are more difficult/costly or may even be impossible to employ.

Vulnerabilities prevalent in state-of-the-art Cloud offerings

Although Cloud Computing is a relatively young topic, there already are myriads of Cloud offerings on the market. Hence, the three indicators of Cloud specific vulnerabilities presented above can be complemented with a fourth, empirical indicator: if a vulnerability is prevalent in state-of-the-art Cloud offerings, it must be regarded as Cloud specific.

Obviously, most such vulnerabilities should also fit one of the other three indicators. Indeed, the following examples are also typical for the core technology web applications and services:

Insufficient/faulty authorization checks

If the implementation of an application carries out insufficient or faulty authorization checks, then service/application users may be able to view information or carry out actions for which they are not authorized. For example, missing authorization checks are the root cause of URL-guessing attacks in which users modify URLs so that they point to information regarding a different user account – missing authorization checks then allow the user to view content of a different user. Security assessments of current Cloud Computing offerings show that faulty/missing authorization checks occur frequently in state-of-the-art Cloud SaaS offerings.

Injection vulnerabilities

Injection vulnerabilities are exploited by manipulating input to a service/application so that parts of the input are interpreted and executed as code against the intentions of the programmer. Examples of injection vulnerabilities are:

- SQL injection: the input contains SQL code that is erroneously executed in the database back end
- Command injection: the input contains OS commands that are erroneously executed via the operating system
- Cross-site scripting: the input contains Javascript code that is erroneously executed by a victim's browser.

Security assessments of web components of current Cloud offerings show the prevalence of injection vulnerabilities in state-of-the-art offerings.

Weak authentication schemes

Many widely used authentication mechanisms are weak. For example, the use of usernames and passwords for authentication is weak because of (1) insecure user behavior (users tend to use weak passwords, re-use passwords, etc.) and (2) inherent limitations of one-factor authentication mechanisms. The implementation of authentication mechanisms may also have weaknesses allowing, for example, the interception and replay of credentials.

The majority of current web applications used in state-of-the-art Cloud services employ usernames and passwords as authentication mechanisms.

Mapping vulnerabilities to controls

Having identified Cloud specific vulnerabilities, a Cloud specific risk assessment can further be supported by identifying security controls that can be used to counter these vulnerabilities. This mapping of vulnerabilities to controls should be based on existing control frameworks such as NIST's report SP800-53 recommended security controls for federal information systems [3] or the information security standard ISO 27002 [5]. As an example, Figure 5 gives an overview of the 17 control families described by NIST SP800-53 – each of these control families contains descriptions of controls related to the security functionality of the family.

Mapping of a Cloud specific vulnerability to mitigating controls should consist of a list of relevant controls and a brief description of why each control is relevant.

Revisiting the "Injection Vulnerabilities" described in the previous section, a mapping to NIST controls could look like this:

When programming web applications/services, sound security engineering principles must be used (SA-08) and security must be embedded into the development lifecycle (SA-03); tests should be performed during development (SA-11) and possibly complemented with a security assessment (CA-02).

Technical means to prevent injection vulnerabilities are information input validation (SI-10) and flow control on user-input (AC-04); depending on the way flow control is implemented, tagging with security attributes (AC-16) of user input may be necessary.

List of NIST SP800-53 controls:

- AC-04 information flow enforcement
- AC-16 security attributes
- CA-02 security assessments
- SA-03 life cycle support
- SA-08 security engineering principles
- SA-11 developer security testing
- SI-04 information system monitoring
- SI-10 information input validation

Identifier	Family
AC	Access control
AT	Awareness and training
AU	Audit and accountability
CA	Security assessment and authorization
CM	Configuration management
CP	Contingency planning
IA	Identification and authentication
IR	Incident response
MA	Maintenance
MP	Media protection
PE	Physical and environmental protection
PL	Planning
PS	Personnel security
RA	Risk assessment
SA	System and service acquisition
SC	System and communications protection
SI	System and information integrity
PM	Program management

Figure 5: Overview of NIST SP800-53 control families.

Putting it all together

Current publications about Cloud Computing security often present the following problems:

- Not every issue that is raised is really specific to Cloud Computing, which makes it hard to determine the "delta" that Cloud Computing really adds with respect to security issues
- The quality of advice about "things to do" or especially important controls is often hard to assess, because proper risk analysis is missing. Which vulnerabilities are mitigated by such advice and how relevant are they really? Are there relevant vulnerabilities that have been overlooked? The very same questions arise when carrying out a Cloud specific risk assessment for a given Cloud service.

Carrying out the steps described above, Atos has identified around 40 Cloud specific vulnerabilities (nine of which are control challenges), and mapped these vulnerabilities to mitigating controls out of NIST's recommended security controls for federal information systems [3]. Furthermore, each vulnerability has been positioned in relevant layer(s) and supporting function(s) of the Cloud reference architecture. Thus, a cloud-specific risk assessment following, e.g. the steps outlined in Figure 2 is supported as follows:

System characterization

By positioning relevant system components in the Cloud reference architecture, a standardized abstract view on a system under evaluation can be achieved.

Vulnerability identification

Because all identified Cloud specific vulnerabilities have also been positioned in the Cloud reference architecture, it is immediately clear, which vulnerabilities are relevant for the system under consideration (and which system components may be affected). Thus, the usually time-consuming process of vulnerability identification can be carried out very efficiently.

Control analysis and control recommendations

The mapping of vulnerabilities into controls provides a sound basis for control analysis and control recommendations.

Atos has created this framework as the basis of a well-founded approach to assessing and treating Cloud related risk. Comprehensive assessments based on this research are currently carried out in the Atos development process to ensure transparency and an adequate level of protection for our customers.

Outlook

Cloud Computing is in constant development. We are certain that additional Cloud-specific vulnerabilities will be identified; other vulnerabilities will become less of an issue as the field of Cloud Computing matures. Using a precise definition of what constitutes a vulnerability as provided by The Open Group's risk taxonomy [4], and the four indicators of Cloud specific vulnerabilities identified in this white paper, will provide a level of precision and clarity that the current discourse about Cloud-Computing security often lacks.

The kind of vulnerability termed "control challenge" in this paper is of special interest for further research into Cloud Computing security: control challenges point to situations where security controls that have been successfully used for many years cannot be effectively used in a Cloud setting. Indeed, many current developments in Cloud Computing, such as the development of security metrics as carried out by a working group of the Cloud Security Alliance (CSA), or the move towards virtualized network components, directly address some of the control challenges identified in this report.

Finally, an analysis of mappings of Cloud specific vulnerabilities to security controls can provide information about which security controls are especially relevant for Cloud computing infrastructures, which is a first stepping stone towards Cloud specific certification and audit schemes.

Sources

1 European Network and Information Security Agency (ENISA), Cloud Computing: Benefits, risks and recommendations for information security, November 2009

2 Gary Stonebruner, Alice Goguen, and Alexis Feringa, eds., NIST SP 800-30: Risk Management Guide for Information Technology Systems, July 2002, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

3 NIST, NIST SP800-53 rev 3: Recommended Security Controls for Federal Information Systems and Organizations, August 2009, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf.

4 The Open Group, Risk Taxonomy, January 2009, http://www.opengroup.org/onlinepubs/9699919899/toc.pdf

5 International Organization for Standardization, ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management, Geneva, Switzerland, 2005

6 Lamia Youseff, Maria Butrico, und Dilma Da Silva, Towards a Unified Ontology of Cloud Computing, in Proceedings of Grid Computing Environments Workshop (GCE), 2008, http://www.cs.ucsb.edu/%7Elyouseff/CCOntology/CloudOntology.pdf

7 International Organization for Standardization, ISO/IEC 27005:2007 Information technology – Security techniques – Information security risk management, Geneva, Switzerland, 2007

8 Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, 2009, http://www.cloudsecurityalliance.org/csaguide.pdf

9 Peter Mell and Tim Grance, Effectively and Securely Using the Cloud Computing Paradigm (v0.25), NIST, 2009, http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

Contact

Jordan Janeczko

Global SI Cloud Strategy: jordan.janeczko@atos.net

About Atos

Atos is an international information technology services company with annual 2010 pro forma revenues of EUR 8.6 billion and 74,000 employees in 42 countries. Serving a global client base, it delivers hi-tech transactional services, consulting and technology services, systems integration and managed services. With its deep technology expertise and industry knowledge, it works with clients across the following market sectors: Manufacturing, Retail, Services; Public, Health & Transport; Financial Services; Telecoms, Media & Technology; Energy & Utilities.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. It is the Worldwide Information Technology Partner for the Olympic Games and is quoted on the Paris Eurolist Market. Atos operates under the brands Atos, Atos Consulting and Technology Services, Atos Worldline and Atos Worldgrid.
For more information, visit: atos.net

For more information, contact: dialogue@atos.net or visit: www.atos.net/security or www.atos.net/cloud

atos.net