enisa
European Network
and Information
Security Agency

Cloud computing: benefits, risks and recommendations for information security

Cloud computing is a new way of delivering computing resources, not a *new technology*. Computing services ranging from data storage and processing to software, such as email handling, are now available instantly, commitment-free and on-demand. Since we are in a time of belt-tightening, this new economic model for computing has found fertile ground and is seeing massive global investment. According to IDC's analysis, the worldwide forecast for cloud services in 2009 will be in the order of $17.4bn[1]. The estimation for 2013 amounts to $44.2bn, with the European market ranging from €971m in 2008 to €6,005m in 2013 [2].

The key conclusion of ENISA's 2009 paper on *Cloud Computing: benefits, risks and recommendations for information security*[3] is that the cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defences can be more robust, scalable and cost-effective. ENISA's paper allows an informed assessment of the security risks and benefits of using cloud computing - providing security guidance for potential and existing users of cloud computing.

The new economic model has also driven technical change in terms of:

Scale: commoditisation and the drive towards economic efficiency have led to massive concentrations of the hardware resources required to provide services. This encourages economies of scale - for all the kinds of resources required to provide computing services.

Architecture: optimal resource use demands computing resources that are abstracted from underlying hardware. Unrelated customers who share hardware and software resources rely on logical isolation mechanisms to protect their data. Computing, content storage and processing are massively distributed. Global markets for commodities demand edge distribution networks where content is delivered and received as close to customers as possible. This tendency towards global distribution and redundancy means resources are usually managed in bulk, both physically and logically.

Given the reduced cost and flexibility it brings, a migration to cloud computing is compelling for many SMEs. However, the survey undertaken as part of ENISA's report (see Survey - An SME Perspective on Cloud Computing[4]) confirms that major concerns for SMEs migrating to the cloud include the confidentiality of their information and liability for incidents involving the infrastructure.

[1] **IDC** *Cloud Computing 2010 - An IDC Update,* Frank Gens, Robert P Mahowald, Richard L Villars, Sep 2009 - Doc # TB20090929, 2009

[2] *Western European Software-as-a-Service Forecast,* 2009–2013, David Bradshaw, Apr 2009 - Doc # LT02R9, 2009

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

[4] http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey

Governments are also interested in the possibility of using cloud computing to reduce IT costs and increase capabilities. For example, the US government GSA (General Services Administration) now offers a portal for cloud computing services[5]. Governments too, have serious hurdles to overcome - in terms of public perception of the secure processing of citizens' personal information in cloud computing infrastructures. On top of this, there are also legal and regulatory obstacles which prevent many eGovernment applications from moving to cloud services. Nevertheless, both governments and SMEs face the reality that many of their employees will be using cloud-based services whether or not this is part of their official policy.

Finally, it is important to note that cloud computing can refer to several different service types, including Application/Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The risks and benefits associated with each model will differ and so will the key considerations in contracting for this type of service. The following sections attempt to make the distinction when the risks or benefits apply differently to different cloud models.

TOP RECOMMENDATIONS

ASSURANCE FOR CLOUD CUSTOMERS

Cloud customers need assurance that providers are following sound security practices in mitigating the risks facing both the customer and the provider (e.g., DDoS attacks). They need this in order to make sound business decisions and to maintain or obtain security certifications. An early symptom of this need for assurance is that many cloud providers are swamped with requests for audits.

For this reason, ENISA has created a standard checklist of questions which can be used to provide or obtain assurance [6].

Documents based on the check-list should provide a means for customers to:

1. assess the risk of adopting cloud services;
2. compare different cloud provider offerings;
3. obtain assurance from selected cloud providers;
4. reduce the assurance burden on cloud providers.

The security check-list covers all aspects of security requirements including legal issues, physical security, policy issues and technical issues.

[5] **General Services Administration US - GSA** [Online] http://www.gsa.gov/Portal/gsa/ep/contentView.do?pageTypeId=8199&channelId=-24825&P=&contentId=28477&contentType=GSA_BASIC

[6] http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework

LEGAL RECOMMENDATIONS

Most legal issues involved in cloud computing will currently be resolved during contract evaluation (i.e., when making comparisons between different providers) or negotiations. The more common case in cloud computing will be selecting between different contracts on offer in the market (contract evaluation) as opposed to contract negotiations. However, opportunities may exist for prospective customers of cloud services to choose providers whose contracts are negotiable

Unlike traditional Internet services, standard contract clauses may deserve additional review because of the nature of cloud computing. The parties to a contract should pay particular attention to their rights and obligations related to notifications of breaches in security, data transfers, creation of derivative works, change of control, and access to data by law enforcement entities. Because the cloud can be used to outsource critical internal infrastructure, and the interruption of that infrastructure may have wide ranging effects, the parties should carefully consider whether standard limitations on liability adequately represent allocations of liability, given the parties' use of the cloud, or responsibilities for infrastructure.

Until legal precedent and regulations address security concerns specific to cloud computing, customers and cloud providers alike should look to the terms of their contract to effectively address security risks.

LEGAL RECOMMENDATIONS TO THE EUROPEAN COMMISSION

In its report, which contains an extended annexe on legal issues, ENISA recommends that the European Commission study or clarify the following:

- certain issues related to the Data Protection Directive and the recommendations of the Article 29 Data Protection Working Party;
- cloud providers' obligation to notify their customers of data security breaches;
- how the liability exemptions for intermediaries arising from the eCommerce Directive articles 12-15 apply to cloud providers;.
- how best to support the creation of minimum data protection standards and privacy certification schemes common across all the member States.

RESEARCH RECOMMENDATIONS

ENISA's report also recommends priority areas of research in order to improve the security of cloud computing technologies. The following are the categories considered, with a few examples of specific areas from the full list:

BUILDING TRUST IN THE CLOUD

- Effects of different forms of breach reporting on security
- End-to-end data confidentiality in the cloud and beyond
- Higher assurance clouds, virtual private clouds etc

DATA PROTECTION IN LARGE SCALE CROSS-ORGANIZATIONAL SYSTEMS

- Forensics and evidence gathering mechanisms.
- Incident handling - monitoring and traceability
- International differences in relevant regulations including data protection and privacy

LARGE SCALE COMPUTER SYSTEMS ENGINEERING

- Resource isolation mechanisms - data, processing, memory, logs etc
- Interoperability between cloud providers
- Resilience of cloud computing. How can cloud improve resilience?

TOP SECURITY BENEFITS

ENISA's report outlines both security benefits and security risks resulting from migration to cloud computing. Below is a summary of the benefits:

SECURITY AND THE BENEFITS OF SCALE: put simply, all kinds of security measures are cheaper when implemented on a larger scale. Therefore the same amount of investment in security buys better protection. This includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances and hypervisors, etc. Other benefits of scale include: multiple locations, edge networks (content delivered or processed closer to its destination), timeliness of response, to incidents, threat management.

SECURITY AS A MARKET DIFFERENTIATOR:security is a priority concern for many cloud customers; many of them will make buying choices on the basis of the reputation for confidentiality, integrity and resilience of, and the security services offered by, a provider. This is a strong driver for cloud providers to improve security practices.

STANDARDISED INTERFACES FOR MANAGED SECURITY SERVICES: large cloud providers can offer a standardised, open interface to managed security services providers. This creates a more open and readily available market for security services.

RAPID, SMART SCALING OF RESOURCES: the ability of the cloud provider to dynamically reallocate resources for filtering, traffic shaping, authentication, encryption, etc, to defensive measures (e.g., against DDoS attacks) has obvious advantages for resilience.

AUDIT AND EVIDENCE-GATHERING: cloud computing (when using virtualisation) can provide dedicated, pay-per-use forensic images of virtual machines which are accessible without taking infrastructure off-line, leading to less down-time for forensic analysis. It can also provide more cost-effective storage for logs allowing more comprehensive logging without compromising performance.

MORE TIMELY, EFFECTIVE AND EFFICIENT UPDATES AND DEFAULTS: default virtual machine images and software modules used by customers can be pre-hardened and updated with the latest patches and security settings according to fine-tuned processes; IaaS cloud service APIs also allow snapshots of virtual infrastructure to be taken regularly and compared with a baseline. Updates can be rolled out many times more rapidly across a homogenous platform than in traditional client-based systems that rely on the patching model.

BENEFITS OF RESOURCE CONCENTRATION: Although the concentration of resources undoubtedly has disadvantages for security [see Risks], it has the obvious advantage of cheaper physical perimiterisation and physical access control (per unit resource) and the easier and cheaper application of many security-related processes.

TOP SECURITY RISKS

The most important classes of cloud-specific risks identified ENISA's paper are:

LOSS OF GOVERNANCE: in using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues which may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences.

LOCK-IN: there is currently little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment. This introduces a dependency on a particular CP for service provision, especially if data portability, as the most fundamental aspect, is not enabled..

ISOLATION FAILURE: multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks). However it should be considered that attacks on resource isolation mechanisms (e.g.,. against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional OSs.

COMPLIANCE RISKS: investment in achieving certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to the cloud:

- if the CP cannot provide evidence of their own compliance with the relevant requirements
- if the CP does not permit audit by the cloud customer (CC).

In certain cases, it also means that using a public cloud infrastructure implies that certain kinds of compliance cannot be achieved (e.g., PCI DSS [7]).

MANAGEMENT INTERFACE COMPROMISE: customer management interfaces of a public cloud provider are accessible through the Internet and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

DATA PROTECTION: cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to

[7] **PCI Security Standards Council** [Online] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place, e.g., SAS70 certification.

INSECURE OR INCOMPLETE DATA DELETION: when a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients. In the case of multiple tenancies and the reuse of hardware resources, this represents a higher risk to the customer than with dedicated hardware.

MALICIOUS INSIDER: while usually less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include cloud provider system administrators and managed security service providers.

NB: The risks of using cloud computing should be compared to the risks of staying with traditional solutions, such as desktop-based models. To facilitate this, in the main document we have included estimates of relative risks as compared with a typical traditional environment.

Please note that it is often possible, and in some cases advisable, for the cloud customer to transfer risk to the cloud provider; *however not all risks can be transferred*: If a risk leads to the failure of a business, serious damage to reputation or legal implications, it is hard or impossible for any other party to compensate for this.

Conclusion

For cloud computing to reach the full potential promised by the technology, it must offer solid information security. ENISA’s paper explains, based on concrete scenarios, what cloud computing means for network and information security, data protection and privacy. We look at the security benefits of cloud computing and its risks. It covers the technical, policy and legal implications. Most importantly, it makes concrete recommendations on how to address the risks and maximise the benefits.