security and cloud computing over a coffee

Business
Services

orange™

editorial

Only a few years after being created, cloud computing is now everywhere. However, if there's no security, there's no cloud computing – for once (!) the market agrees on this point. There are numerous questions and uncertainties : what is "new" about the security of cloud computing? What about the human aspect of the cloud computing security equation? Where do you start and which references should you use when initiating your cloud project? The booklet you are currently holding contains a selection of articles you can read over a coffee that will give you a better idea of the "security of cloud computing."

I hope you enjoy it and I hope to see you soon on our blogs, where the adventure continues!

Jean-François Audenard

summary

the invasion of cloud services in businesses : what should you do?

by Jean-François Audenard

For companies, cloud computing is a small revolution in how computing is viewed but also fresh cause for concern, in the same way as those infections that take root between your toes : they crop up, you treat them and you think they've disappeared, until they resurface a little while later...

For businesses, cloud computing applications are more or less the same thing as athlete's foot or other fungi : **employees sign up for cloud services on their own accord**, without informing the security manager; in fact, the latter is deliberately left out of the loop : it wouldn't do for them to go poking around in things that are none of their business.

According to Doug Toombs, Senior Analyst at Tier1 Research this change must be supervised as it is now too late to stop it.

underlying motivation : quick to implement, documentation and costs

For corporate departments, improving productivity and flexibility is all about being more responsive when implementing the necessary resources and systems for achieving their objectives. For years (or even decades) now, IT departments have been imposing unrealistic deadlines combined with costs worthy of the most extravagant swindle.

good to know

Signing up for cloud services is quick and easy : all you have to do is go to the website and enter your corporate credit card information.

Another reason is the fact that there is no equivalent of external cloud services within the company. Alternatively, those **external services are simply better documented and clearer than their internal equivalents**. Admittedly, some internal services are of good quality, but the documentation for them is often a bit scant, out of date or even virtually obsolete... and woe to anyone who speaks up and says what everybody is thinking anyway!

Before the arrival of the cloud, company departments were (pardon the expression) a little “incestuous.” Thanks to cloud computing, they now have a choice : IT departments will thus have to adapt and evolve, and security departments will, too.

a matter of fact, a trend that cannot be stopped

Signing up for cloud services is quick and easy : all you have to do is go to the website and enter your corporate credit card information. The most popular cloud services fall into the categories SaaS (Software as a Service), PaaS (Platform as a Service) or even IaaS (Infrastructure as a Service).

Rather than cutting off internet access (completely unrealistic) or filtering access to cloud services (when will we see a “cloud services providers” option in URL filtering systems?), **the trend is more towards utilizing an increasing number of IT service providers**. IT and security departments are thus obliged to keep up with this trend and monitor it if they want to maintain their status and continue to be respected.

warning

it is important to ensure that data can be properly recovered in a reusable format

prepare and be ready for the future

IT departments, assisted by security departments, must take a balanced view of things and provide guidance for their companies during this transition towards cloud computing. Without wanting to rub anyone the wrong way, my opinion is that security departments are more used to "accompanying" projects than IT departments are. Using cloud services without thinking things through can indeed be dangerous for a company. There are two keywords here : conformity and continuity.

personal data

French companies that process data are required to ensure that data remains secure and stays within the borders of the European Union (or within the territory of a country recognized as offering "sufficient protection"). Since not everyone is aware of these regulatory requirements (European Directive 95/46/EC), security departments have a legitimate role to play in steering a company (without trying to oppose it or necessarily seek to implement other solutions) towards a supplier capable of meeting this need to ensure data remains within a predetermined list of countries.

Similarly, it should be ensured that the service provider's technical support teams are located in familiar countries. And it's not only the data that must be located in specific data centers - the persons accessing that data remotely must also be in known locations.

good to know

French law states that the end client must be informed when personal data concerning him is liable to leave Europe.

French law states that the end client must be informed when personal data concerning him is liable to leave the European zone (or a "recognized" country), and this must be set out in the service agreement.

continuity

Services such as PaaS for applications or to operate virtual machines in the cloud are often used because of the rapidity of their implementation, to meet occasional spikes in workload or to speed up developments or tests. For each of these scenarios in which cloud services are used, it is essential to ensure that the activities in question can be shifted to a different supplier from the one originally selected (if the original supplier were to cease trading, for example). Similarly, a company can begin a project using the cloud services of a third party and then 're-internalise' the project to a private or community cloud.

reversibility

If reversibility issues are not addressed and resolved during the initial phase of subscribing to the service, going back to them later may be prohibitively complicated and in some cases impossible. In any event, it is important to ensure that data can be successfully recovered in a reusable format. For IaaS, this is done by including the option of recovering full back-ups of the virtual machines involved (in a hypervisor-specific format or alternatively as OVF files). The issue is not a new one with regard to PaaS – the statements recently exchanged between Google and Joyent ("Google Cloud Services Criticized by Jason Hoffman", 21 August 2011) about Big Table are a good example of using standardised (or at least non-proprietary) techniques, to avoid the otherwise inevitable "locked-in syndrome."

flexibility and accompaniment

The ball is in the court of IT and security departments : cloud computing is here to stay and is set to become even more widespread, as it offers these departments the agility they need. The Japanese proverb “Snow never breaks the willow’s branches” is a good illustration of the behaviour to adopt : flexibility and accompaniment are the keys to a successful transition to cloud computing.

the article online

the invasion of cloud services in businesses : what should you do?

understanding cloud data protection

by Jean-François Audenard

Data stored in the cloud must be protected against unauthorized access and changes. The more secure and comprehensive the protection, the more data volume and variety can increase.

While articles on this topic abounds, it is often quite confusing and fragmented so I've wanted to share a few ideas with you on the subject.

The lifecycle of data is a constant that can prove a particularly useful tool for any kind of cloud service. However, **things can get complicated for certain lifecycle phases** depending on the kind of service. Different data security methods are used for Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

life cycle of data : reference model

data lifecycle

The lifecycle of data in a cloud breaks down into five major steps : data is transferred to the cloud, stored there, used, recovered and eventually destroyed. At each step, different access control and encryption measures can be taken to ensure data security.

the foundation : access control

Data access is controlled using authorization mechanisms : a person (or system/program) has to present his/her credentials in order to access data. All techniques, systems and means of controlling access fall under **Identity and Access Management** (IAM). As IAM is a very broad topic, I suggest we put it aside for now.

data transfer : everything's under control

Sending data from a company's internal systems to the cloud and retrieving it are the best-protected steps. The company can either **encrypt data** internally and then send it, or use transport layer security with encryption. In the latter category, the Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL) protocols are quite widespread. Combined with **authentication** based on asymmetric keys (public-key cryptography, for example), these protocols make it possible to transmit data to or from the cloud in total security. This is a comfort zone with existing standards and reliable, easy-to-use systems.

things get tricky with data storage

Once sent to the cloud, data is stored there. In the absence of any recognized standard, the use of encryption depends entirely on the service provider, and it is not always clear how their systems operate. To ensure data remains available when stored in the cloud (as in BaaS – Backup as a Service), it is best to **encrypt it before transfer**. Cloud customers have to carry out this process on their own (or use tools made available by their service provider).

Obviously, in the case of SaaS, only the service provider can handle encryption; the end-user has a nearly non-existent role and therefore virtually no control. IAM is even more critical here than in the case of BaaS, where encryption can be performed at the source.

select first and foremost a supplier you can trust and who is familiar with your requirements and restrictions

warning

Though it may not be a walk in the park, there are several solutions available for “at rest” or stored data. The situation is even more complicated for data that needs to be used in the cloud.

no standards for data used in the cloud

No solution currently exists for data that must be used in the cloud where it is stored. Let’s take the example of a virtual machine (VM) deployed in an IaaS cloud. The VM uses a file system to store the operating system, applications and application data. Even if the file system is encrypted, the encryption keys have to be included in the VM for it to work. So if an attacker manages to recover the keys, he/she can access the data on the VM hard disk.

In this case, **data security will depend on the access management measures** put in place for external access and cloud administrators/users. Trusting your service provider thus becomes even more important when it is handling your VMs. The same goes for any cloud application (webmail, customer relationship management applications, document management, etc.).

encryption : a key ally in data destruction

Once data has been recovered from the cloud, it’s important to make sure that it disappears completely. You have to ask your service provider about its data deletion policies, resources, and procedures. However, doubt can still persist, which is when encryption can lend a helping hand.

Without the decryption key, pre-encrypted data is entirely worthless : so to destroy data, simply **throw the encryption key away**. This ensures that data remains inaccessible even if your cloud provider puts the key under the doormat without warning.

the importance of a trusted service provider

Methods for securing data in the cloud still leave much to be desired (except for those used during transfer). Until standards are developed and implemented by service providers, trusting your own provider is absolutely essential. Trust is gained over time and must be maintained; rather than taking a giant leap into the unknown, I recommend that you **choose a service provider you trust**, who knows your needs and constraints. At the same time, never err on the side of blind trust. A tight contract and a meticulous, in-depth analysis of the provider's security practices are required steps in the selection process.

the article online
understanding cloud
data protection

cloud IaaS : 15 recommendations for secure servers

by Jean-François Audenard

IaaS (Infrastructure as a Service) is perhaps the first type of cloud service to come to people's minds. This could be because this level of service benefits from the "halo" of virtualisation...

In IaaS arrangements, the client subscribes to a hosting service for an operating system running in a virtualised environment. Once the system has been delivered by the service provider, it is up to the client to secure it. The scope of this security process will depend on the client's requirements and on what is and is not delivered by the service provider.

Let's assume that the IaaS service you've just taken out is entry level. It's up to you to put in the hard work to reinforce security to an adequate level.

good to know

You should begin by identifying your security requirements, then select your supplier and add what the supplier does not provide.

warning

do not store your decryption keys in the system : they must not be entered except during the decryption process

I will give you 15 recommendations for securing a virtual machine within a IaaS cloud

1. Encrypt all network traffic
2. Make sure that each system can support only one service at a time (*)
3. Consolidate the security of your operating system (Microsoft MBSA, Bastille Linux, etc.)
4. Activate the encryption functions built into file systems or peripherals at block level
5. Encrypt all data placed in storage spaces (SAN, NAS, etc.)
6. Do not store your decryption keys on the system : they must not be entered except during the decryption process
7. Keep the number of network ports open on each system to a minimum
8. Install corrective security patches regularly, on both the operating system and the applications
9. Systematically scan for vulnerabilities
10. With the exception of public services like HTTP/HTTPS, limit the number of source IP addresses authorised to connect
11. Avoid using passwords for access in console mode – use RSA keys or client SSL certificates instead
12. Back up your data on a regular basis, retrieve those backups and store them in a secure location
13. Install an intrusion detection system in the operating system (e.g. OSSEC, CISCO CSA, etc.)
14. If you have reason to suspect an intrusion, take a snapshot of the system and stop there (*)
15. Develop your applications securely (OWASP)

Normally, you should begin by identifying your security requirements and then selecting your supplier(s) and providing yourself what they do not offer, whether in terms of the standard service level or with regard to options.

I'm not reinventing the wheel here : an IaaS server is fairly similar to a dedicated server hosted with a service provider – remove the virtualisation layer and you'll find yourself in more or less familiar territory. Of these 15 recommendations, only two (*) require techniques associated with virtualisation.

PS : none of this is insurmountable for an experienced system/security administrator, especially since virtualisation means that copying and pasting virtual systems has a degree of industrialisation unseen in dedicated servers. Happy clouding!

the article online

IaaS cloud : 15 recommendations
for secure servers

Forrester: security in cloud services in the spotlight

by Jean-François Audenard

In a Forrester study entitled “Status, Challenges, And Near-Term Tactics For Cloud Services In Enterprise Outsourcing Deals” (Paul Roehrig, November 18, 2009), issues relating to the security of cloud services are discussed extensively.

Before companies take the “giant leap” towards cloud services, 7 major questions will need to be answered by cloud service providers. **The most important issue is security** : “Even so, perceptions and genuine technical hurdles put security as one of the biggest challenges to broader enterprise cloud services adoption”.

The security of cloud services is highlighted as a recurring issue on which positions are clearly conflicting.
Some claim that **security in the cloud is impossible** while others fight the opposite corner tooth and nail : the cloud can be more secure than dedicated infrastructures. These contradictory messages can be explained by the fact that the level of technology and processes implemented in cloud platforms is not as well developed as in other domains. On the other hand, **security for some “cloud” services can properly be described as having reached maturity.**

security for some 'cloud' services can properly be described as having reached maturity

warning

Personally I would agree with their analysis : you only have to look at mail services. Big companies subcontract (entirely or in part) their electronic communications to service providers. This actually works pretty well.

To draw a parallel : in the cloud, you sometimes encounter terms like **“private cloud,” “public cloud” or even “community cloud”.** Opposite each of these, place a “dedicated hosted mail platform,” “Gmail” or “electronic messaging services for the business sector” (stay with me here). Each of these “cloud” services can be provided in a secure manner, at the level of functionality and price that people expect.

What does Forrester recommend? It’s pretty simple : “integrate security as one of the strategic choices and as part of the selection process.”

This comes as no surprise : since companies cannot outsource their risks (they can arguably transfer them, but at a cost), they have to rely on their security experts to assess the security claims made by their cloud service providers.

“Security needs to be a part of the project from the beginning.” Nothing new under the sun here. Does this happen as a matter of course? Each individual business is responsible for ensuring it does.

PS : I have deliberately omitted mentioning everything that has nothing to do with security. The document from Forrester does not focus uniquely on security.

the article online

Forrester : the security of cloud services in the spotlight

three cloud computing security references

by Jean-François Audenard

Here are three documents that I consider to be references in cloud computing security (or, more generally, in the field of information systems security outsourcing).

#1
Cloud Security Alliance, "Security Guidance for Critical Areas of Cloud Computing Version 3.0"

(177 pages)

This is the heavyweight of the list. Published by the Cloud Security Alliance, the dense "Security Guidance for Critical Areas of Cloud Computing Version 3.0" is the "reference of references" for any professional in the field.

This document contains all of the latest information on cloud computing security. My only critique is that some of the security measures it describes are a bit too theoretical and complicated to be useful to everyone.

Of course, this is only the tip of the iceberg. The Cloud Security Alliance has published many other documents. Check out their website, you won't be disappointed!

#2 European Network and Information Security Agency (ENISA), “Cloud computing : benefits, risks and recommendations for information security”

(125 pages)

This comprehensive document comes from ENISA, the European agency devoted to information systems security. In “Cloud computing : benefits, risks and recommendations for information security”, ENISA thoroughly analyzes the risks associated with cloud computing and suggests appropriate safety measures to address them.

The easy-to-understand guide presents each risk in the same summary format. If you’re just learning the ropes, this is the document for you. Go directly to page 9 to learn about the top eight cloud-specific risks.

#3 Payment Card Industry Security Standards Council, “PCI DSS Virtualization Guidelines Version 2.0”

(39 pages)

The Payment Card Industry Data Security Standard (PCI DSS) sets the rules for payment card information security. The interesting thing about PCI DSS is that the rules (or “security objectives”) are prices and known in advance. As you might expect, these rules are very strict.

The PCI DSS Virtualization Guidelines clearly explain what to set up on a virtualization layer. To learn how to secure your hypervisor, this document is all you need, since it covers both technical and organizational aspects.

my favorite

My preferred reference is the guide by the Cloud Security Alliance. It’s a state-of-the-art review of cloud computing security.

what are your favorite references?

I have intentionally left out specific technology guides and documents produced by the National Institute of Standards and Technology, the National Security Agency, and others.

Which documents are your go-to references? I invite you to share the hidden gems you’ve stashed away on your hard drives and other online sharing platforms.

the article online
3 reference documents on security in cloud computing

the author

Jean-François Audenard

Within Orange Business Services, I am responsible for incorporating security at the heart of our product range and cloud computing services. I am passionate about what I do and take a holistic, committed approach to my work – I'm never one to sit on the fence. I am a committed and enthusiastic blogger and enjoy charting new territory and "breaking the mold". Honesty is my speciality and optimism and willpower are my driving forces.

Our blog :
http ://blogs.orange-business.com/connecting-technology/

Document available for download at :
http ://knowledge-center.orange-business.com/

Edited by Orange Business Services
10.09.2012

security and cloud computing **over a coffee**

France Télécom – 78, rue Olivier de Serres, 75015 Paris, France – SA au capital de 10 595 541 532 – 380 129 866 RCS Paris – Document non contractuel – juin 2012

Business
Services

orange™