enisa
European Network
and Information
Security Agency

Critical Cloud Computing

A CIIP perspective on cloud computing services

Version 1,0, December 2012

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Author

Dr. M.A.C. Dekker

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

The overview of cloud uptake and outages was produced in collaboration with Dr. Srijith Nair, as part of the ENISA framework for experts, and Analysys Mason as part of the ENISA tender P/04/12/TCD.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Executive summary

Public and private sector organisations are switching to cloud computing. While some years ago applications would be mainly run on servers on their own premises or dedicated data centres, now applications are outsourced to large cloud service providers and run in a few large data centres. Public data on the uptake of cloud computing shows that in a couple of years around 80% of organisations will be dependent on cloud computing. Large cloud providers will be serving tens of millions of end-users.

From a CIIP perspective this concentration of IT resources is a *'double edged sword'*: On the one hand, large cloud providers can deploy state of the art security and resilience measures and spread the associated costs across the customers. On the other hand, if an outage or a security breach occurs the consequences could be big, affecting a lot of data, many organizations and a large number of citizens, at once. In fact in the last year there were a number of outages affecting several very large sites with millions of users.

The EU member states have committed to protecting critical ICT systems via the European Commission's CIIP action plan by preventing large cyber-attacks and cyber disruptions of critical ICT systems. In the follow-up the European commission asks for a discussion about a governance strategy for cloud computing services, in the context of CIIP.

In this report we look cloud computing from a CIIP perspective and we look at a number of scenarios and threats relevant from a CIIP perspective, based on a survey of public sources on uptake of cloud computing and large cyber attacks and disruptions of cloud computing services.

From the scenarios and the data about uptake and incidents we draw a number of conclusions.

- **Cloud computing is critical:** Cloud computing usage is growing and in the near future the vast majority of organizations will rely on some form of cloud computing services. This makes cloud computing services critical in themselves. When cyber attacks and cyber disruptions happen, millions of users are affected. Cloud computing is being adopted also in critical sectors, like finance, energy and transport.
- **Cloud computing and natural disasters:** A key benefit of cloud computing is resilience in the face of regional power cuts or local natural disasters. It is difficult to mitigate the impact of fairly common regional disasters like floods, storms, or earthquakes in a set up with only a single datacentre, or a traditional set-up with a legacy onsite IT deployment.
- **Cloud computing and overloads or DDoS attacks:** Elasticity is a key benefit of cloud computing and this elasticity helps to cope with load and mitigates the risk of overload or DDoS attacks. It is difficult to mitigate the impact of peak usage or a DDoS attack with limited computing resources.
- **Cyber attacks:** Cyber attacks which exploit software flaws can cause very large data breaches, affecting millions of users directly. The impact of cyber attacks is multiplied by the concentration of resources which is a result of the uptake in cloud computing.
- **Infrastructure and platform as a Service the most critical:** The most critical services are large IaaS and PaaS services which deliver services to other IT vendors who service in turn millions of users and organisations.
- **Administrative and legal disputes:** Cloud computing is not immune to administrative or legal issues. If there is a legal dispute involving the provider or one of its customers, than this could have an impact on the data of all the other co- customers (or co-tenants).

The CIIP action plan calls for a discussion about governance strategies for cloud computing and also in speeches about the EU Cyber Security Strategy the issue of cyber security governance is addressed. Below we make a number of recommendations related to the issue of national governance of critical cloud computing services.

Governance, from a national perspective, can be split into three key processes: 1) Risk assessment, 2) ensuring that appropriate security measures are taken, and 3) collecting incident reports.

- **Risk assessment:** Risk assessment is the basis for security governance.
  - Assets in scope: It is important to take a pragmatic approach and address the most critical cloud computing services first. It is easy to say that 'all cloud computing services are critical' but it is infeasible to address everything at once. As mentioned, since outages at IaaS or PaaS providers can have an impact across a range of organizations, this means that they should be treated with priority.
  - Assessing dependencies on cloud computing: Most countries, when making national risk assessments, from a critical infrastructure perspective, take into account power supply and electronic communications networks. Public sources on uptake cloud computing suggest that it is necessary to take into account also large cloud computing services and large datacentres.
  - Transparency about logical and physical dependencies: A risk assessment requires a clear view of the dependencies. It should be clear which critical operators and critical services depend on which cloud computing services. The special nature of cloud computing creates resilience but it can also increase interdependencies and cause cascading failures. Outages at an underlying IaaS or PaaS provider can affect a range of (otherwise unrelated) services across society. It is important to map all the main logical and physical dependencies.
- **Security measures:** Taking appropriate security measures is the focus of security governance.
  - **Foster exchange of best practices to achieve a security baseline:** It goes without saying that it is important that cloud providers take appropriate security measures. These measures should be based on best-practices. It is important for government authorities to support and foster the exchange of such best practices. Security is constantly changing and security measures must be improved continuously. Government authorities should encourage an open culture of exchange and discussion about security measures. Security is about continuous improvement and government authorities should avoid a situation where a specific set of best practices is cast in stone (by regulation or self-regulation).
  - **Logical redundancy:** Cloud computing services are often set-up with several redundant datacentres to withstand outages of single datacentres (due to power cuts or natural disasters, for example). Many cyber attacks, however, capitalise and exploit software flaws, which are persist across the datacentres. It is important to prevent and mitigate the impact of cyber attacks by creating also logical redundancy – that is, to use different layers of defence and to use separate systems with a different logical structure, to cross-check transactions and to detect attacks.
  - **Standardisation:** From a CIIP perspective standardization in cloud computing is very important, because it allows customers to mitigate issues related to a specific provider or a specific platform. Standardization, especially for IaaS and PaaS services, would allow customers to move workload to other providers in case one provider has suffers a large outages caused by system failures or even administrative or legal disputes.

  - **Monitoring, audits, tests, and exercises:** There is a lot of information security literature about the importance of auditing and testing systems. Cloud computing providers should schedule frequent audits and tests, by internal testers and auditors, and, when relevant, by external testers and auditors. In discussions about governance, often the need for certification, by independent external auditors is stressed. But it is hard for an external auditor to assess the security of a complex and continuously changing system, by performing an audit once per year. Cloud computing providers and government authorities should have a continuous program of monitoring, audits, tests and exercises in place. Yearly audits by external parties are only a small part of such a program.
- **Incident reporting:** Incident reporting provides a cross-check on the security measures, it provides the input for an improved risk assessment, and it provides strategic feedback about the overall governance process.
  - **Mandatory reporting:** Without incident reports it is very difficult to understand the impact of security incidents on cloud computing providers. This complicates risk assessment, both for cloud computing service providers, as well as, at a national level, for government authorities like agencies responsible for (civil) contingency planning. Lack of data about incidents makes it very difficult to prioritize security measures, and in this way security governance becomes inefficient or even ineffective. Government authorities and cloud providers should agree on the thresholds for reporting and the type of services that should be in scope.
  - **Legal consequences:** Secondly, it is important to consider that certain cyber attacks are stealthy and their traces may be difficult to spot even for system administrators who know the cloud computing systems inside out. There is always a risk that security incidents are not reported to higher management or to authorities for fear of reprisal or legal consequences. Member states should consider giving incentives to providers who report security breaches which would otherwise go unnoticed.

Table of Contents

1 Introduction

Public and private sector organisations are switching to cloud computing and single cloud service providers sometimes provide services for millions of users and a range of organizations and businesses. This means that also from a CIIP perspective cloud computing becomes relevant. In this paper we look at key risks for cloud computing services from a CIIP perspective. We look at data about the usage and uptake of cloud computing and we analyse some scenarios. We conclude with recommendations for government bodies, like regulators and contingency agencies, about addressing the risks of cloud computing.

Policy context

The EU Member States have committed to protecting CII, via the European Commission's Communication on Critical Information Infrastructure Protection (CIIP)[1]. The CIIP action plan focusses on strengthening the security and resilience of CII, and *preventing large cyber-attacks and cyber disruptions*. The communication mentions cyber attacks, natural disasters and technical failures as the main threats, and cites two examples: the DDoS attacks on Estonia in 2007, and the transatlantic submarine cable cuts in 2008. The communication explicitly calls for discussion about the best governance strategy for cloud computing services in this respect.

Critical information infrastructures (CII) are the ICT systems which are vital for the economy or the society of a country (or a group of countries). There are several definitions of CII in the literature. The European Commission (in the Communication on CIIP) has defined Critical Information Infrastructures as all ICT systems which are either, a) critical infrastructure themselves, or b) essential for the operation of other critical infrastructures. The OECD defined CII as those information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy[2].

The European Commission is also developing a European Cyber Security Strategy. The roadmap for the strategy refers mentions extending Article 13a (a regulation on security and resilience of telecommunications) to other business sectors.

Goal

The goal of this document is to look at the security and resilience of using cloud computing, from a CIIP perspective.

Target audience

This document is targeted at IT officers in government bodies, like regulators and contingency agencies, national and EU level policy makers, and also cloud computing vendors who deliver cloud critical cloud computing services.

Scope

[1] *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF*

[2] *http://www.oecd.org/sti/40825404.pdf*

In this paper we take a national, CIIP perspective. This means that we are primarily focussed on large-scale impact on society (for example caused by large outages or large cyber-attacks). We do not go into details about issues like data protection, legal compliance or governance of individual cloud service contracts and SLAs, for example.

For the full range of security risks and benefits for organisations (SMEs or government organisations) when adopting cloud computing we refer to earlier ENISA papers.

Disclaimer about examples

For the sake of clarification we provide numerous examples, referring to public sources about cloud services, cloud customers, security incidents, and so on. By no means is it our intention to single out individual organizations for praise or criticism.

Structure of this document

In Section 2 we show the uptake of cloud computing, by listing several public sources. In Section 3 we explain the CIIP perspective on cloud computing and in Section 4 we go over a number of specific scenarios, based on public sources about cloud computing usage and passed incidents. In the conclusions we make some key recommendations for mitigating the impact of large failures with critical cloud computing services.

2 Uptake of Cloud Computing

Public and private sector organisations are switching to cloud computing: While years ago software applications were running on servers on their own premises or dedicated data centres, now applications are outsourced to large cloud service providers and run in very large data centres.

Cloud computing is being adopted rapidly across society, and across different sectors of society. Many analysts predict a further growth (of around 30% a year). We give some examples:

- **IDC November 2011**: The total cloud services market in Western Europe alone will grow from 3.3 billion euros in 2010 to 15 billion by 2015, which translates to a 35% growth rate. IDC estimates that by 2014 most organizations will turn to the cloud first to implement new functionality needed.
- **Gartner 2012**: Almost 33% of the organisations polled are either already using or planning to use cloud based SaaS offerings to augment their Business Intelligence functions.
- **AT&T 2011**: According to London-based business_continuity_survey, almost 37% of companies are considering using cloud_technology to help them deal with disruptive events to ensure business continuity.
- **Forrester 2012**: 18% of high-tech industries have already adopted IaaS solutions and as many as 25% plan to adopt them in the near future. In the more regulated sectors like government, financial and health, the uptake is less. For example, in the government sector about 10% has already adopted use of IaaS services, while about 5% plan to use IaaS in the near future. Similar figures are reported for the healthcare and financial services sector.

The public data tells only part of the story - from public data it is difficult to understand how many end-users or organizations depend on a cloud computing provider, because cloud computing providers often offer services to other organisations, which in turn provide services to the (sometimes millions of) customers. For example, a SaaS cloud computing provider who uses the cloud (an IaaS cloud computing provider) for computing and storage resources. This kind of reselling of IT resources makes it hard to estimate how many end-users depend on a single cloud provider and this makes it hard to estimate the full impact of an outage in society. We give some examples:

- **Amazon 2011:** Amazon AWS infrastructure is reported to carry as much as 1% of the all internet consumer traffic in North America and on an average a third of all internet users visit an AWS powered site daily[3]. Amazon reports having customers like Zynga, Animoto, Reddit, MySpace, Netflix, Dropbox, airbnb, Ericssons, European Space Agency, HootSuite, IBM, Mahindra Satyam, Newsweek, UniCredit, Spiegel.Tv, PBS, Yelp, IMDB, Linden Labs, FourSquare, SmugSmug, Alexa, The Guardian, Farmville, Sitepoint, EventBrite.
- **Rackspace 2011:** By the end of 2011 Rackspace reportedly served 172,510 customers, including Transport of London, Virgin Trains, UK MoD, NHS Direct, Fiverr, Pitchfork, The Register, the Royal Navy, and TweetPhoto.

[3] http://blog.deepfield.net/2012/04/18/how-big-is-amazons-cloud/

- **Google 2011:** Google reports that Google Apps customers include US General Services Adminstration, Essilor, Ispen, BBVA Spain, Capgemini, SNL Financials, Salesforce.com, Essence, The Guradian, LSI Logic, The Telegraph, and so on.
- **Microsoft:** Microsoft Dynamics CRM is reported to generate about $500 million from its on-premise and cloud offerings[4]. Its set of customers includes Aer Lingus, Dow Chemicals, Hyatt Hotels, Univ. of Georgia, Los Angeles Community College District etc.

Other companies use cloud computing services as part of private arrangements (private cloud) and these arrangements are not public.

- 92% of IT decision makers at large companies have indicated that they will "definitely or probably" expand their datacentre footprint in 2012[5].
- Global investment in data centre facilities will grow in excess of 16% to top 30 billion euros in 2012[6].

The datacentres used for cloud computing are very large. We give some examples of public cloud providers:

- It is estimated that the Amazon EC2 is powered by half a million blade servers, over 50,000 of which are hosted in the Dublin datacenter[7].
- The new Facebook server farm in the US state of Oregon measures 14000 square meters and cost around 200 million US dollars to build[8].

There are a number of other critical sectors where cloud computing is being adopted. Below we give examples from the finance sector, the transport sector and the energy sector:

- In 2011 Banco Bilbao started using cloud for email and calendar applications. The bank has 100.000 employees across the globe[9].
- In 2011 NYSE Euronext announced the creation of Capital Markets Community Platform, a community cloud for traders, offering on-demand computing resources.
- In 2012 the NASDAQ OMX Group announced the launch of FinQloud, a new cloud computing platform powered by Amazon Web Services and designed for the financial services industry.
- ITA, the air transport IT specialist launched the ATI Cloud, a form of community cloud, for the airline industry to provide a wide range of on-demand business and IT resources that are tailored specifically for the industry. SITA's network connects over 17,000 sites globally and

[4] http://www.marketwatch.com/story/microsoft-cloud-strategy-coming-into-focus-2012-03-12

[5] https://www.datacenterknowledge.com/archives/2012/03/12/cloud-growth-spurs-demand-for-data-centers/

[6] Data Center Dynamics Growth, www.datacenterdynamics.com/research/market-growth-2011-2012

[7] https://huanliu.wordpress.com/2012/03/13/amazon-data-center-size/

[8] http://www.bbc.co.uk/newsbeat/16838342

[9] http://www.pcworld.com/businesscenter/article/247851/spanish_bank_to_move_100000_employees_to_google_apps.html

links with 90% of the world's airlines. The community cloud now runs on 6 datacentres (in Atlanta, Frankfurt, Singapore, Hong Kong, Sydney and Johannesburg)[10].

- ExxonMobil Upstream Services built an IaaS platform to deliver geo-imagery to mobile land exploration workers[11].
- Atmos Energy Corporation, the American distributor of natural gas, deployed a cloud based SaaS solution to bring together utility assets and consolidate operations spread across six business units[Error! Bookmark not defined.].
- Digital Oilfields developed a cloud-based infrastructure to remotely deliver IT services[12].
- According to IDC's 2010 Vertical Group Survey, 10.3% of oil and gas companies were using or implementing cloud computing technologies and 7% had cloud computing on their technology road map. IDC Energy Insights projects that global oil and gas industry investment in public cloud will rise to more than USD 2 billion in 2014[13].

Key Points

The data describing the uptake of cloud computing shows two aspects to take into account:

- Cloud computing usage is growing and in the near future the vast majority of organizations will rely on some form of cloud computing services. This makes cloud computing services critical in themselves – simply because so many organizations and users now use cloud computing on a day to day basis.
- Cloud computing is being adopted also in critical sectors, like finance, energy, transport and even governmental services.

[10] http://www.lightreading.com/document.asp?doc_id=217569

[11] "Six questions every executive in the energy industry should ask about cloud computing" http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Energy_Cloud_Computing_POV.pdf

[12] http://www.rickscloud.com/cloud-benefits-in-the-energy-and-utility-industry/

[13] Oil and Gas: Into the Cloud?, Jill Feblowitz, http://www.spe.org/jpt/print/archives/2011/05/11Management.pdf

3 CIIP Perspective of Cloud Computing

In this document we take a CIIP perspective on the uptake of cloud computing, and we identify the main risks for critical cloud computing services.

3.1 Concentration of ICT resources

Adoption of cloud computing implies a concentration of IT resources in very large datacentres. This is depicted in diagram below (Figure 1), where the squares are (connected) organizations or operators, and the blue areas indicate IT resources. In information security, the concentration of IT resources is a *'double edged sword':* On the one hand, large cloud providers can deploy state of the art security and business continuity measures and spread the associated costs across the customers. On the other hand, if an outage or a security breach occurs then the consequences could be big, affecting many citizens, many organizations, at once. To illustrate this paradox, we look at three past incidents:

- **Resilience:** The Japanese earthquake of 2011 showed how resilient cloud computing can be in the face of disaster and in the aftermath. Cloud services survived power outages by using emergency fuel and data connections over mobile networks and fixed networks held up. Traditional IT deployments in the disaster area on the other hand went offline. In the aftermath of the disaster, cloud service providers provided support for emergency services, and in the recovery phase cloud computing was used by organisation to quickly get services up and running.
- **Single point of failure**
    - Lightning struck in the Dublin region in summer 2011 affecting the cloud services of some major cloud providers. The outage lasted 2 days and affected many of their customers.
    - In summer 2011 a software flaw in a SaaS cloud service product for backups and document storage allowed each user to see documents of millions of other users, for up to 8 hours.

The concentration of IT resources makes cloud computing services critical and relevant to look at from a CIIP perspective.

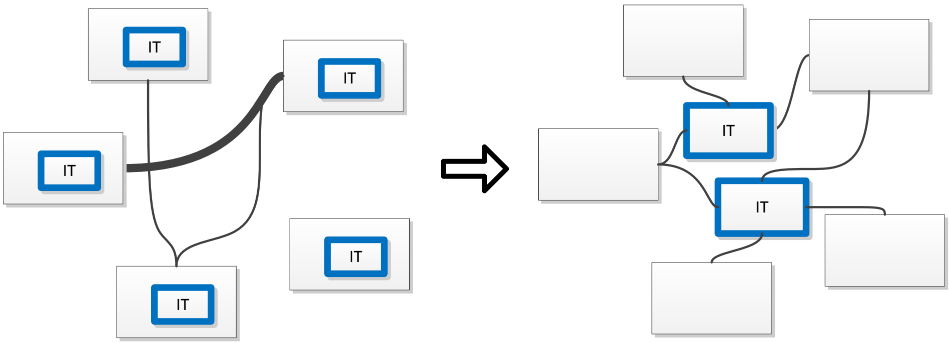

Figure 1. Transition to Cloud Computing from a national perspective

3.2 Cloud and CIIP

Critical information infrastructures (CII) are the ICT systems which are vital for the economy or the society of a country (or a group of countries). There are many definitions of CII in the literature. The European Commission has defined Critical Information Infrastructures as all ICT systems which are either, a) critical infrastructure themselves, or b) essential for the operation of other critical infrastructures. From a CIIP perspective cloud computing service can be critical in two ways:

1. Cloud computing services can be critical in themselves.
2. Cloud computing services can be critical for other critical services

It is not always clear how to distinguish between the two categories. Consider for example an eHealth record platform implemented using cloud computing (users and doctors log in to upload health record data about symptoms and treatment). Obviously the eHealth record platform is critical, but it is not clear if it falls in category 1 (the eHealth record platform is critical in itself) or in category 2 (the eHealth record platform is not critical in itself, but needed for emergency health care, which *is* critical). We refrain from distinguishing between these two cases, and call the cloud computing services in both cases 'critical'.

The CIIP action plan addresses two kinds of large-scale security incidents:

- cyber disruptions (or outage) with a large impact,
- cyber attacks with a large impact We take the same perspective in this document. We go over the two types of incidents[14].

3.2.1 Cyber disruptions

A cyber disruption in this context means (temporary or permanent) loss of service, with impact on users of the cloud service who rely on its continuity. A good example is when critical services, such as emergency care, depend on these cloud services. When looking at these dependencies it is important to distinguish between the different levels of continuity required. Some cloud services can be offline for a day without causing significant impact in society. For other cloud services a couple of hours of downtime is already disastrous. We illustrate continuity dependencies in Figure 2, where we show how different critical assets (like banking/trading), with different continuity requirements (90%, 99%, or 99,9%), may depend on continuity of power, network and cloud services or datacentres.

For example, consider a power outage in a data centre of a telecommunications provider. This could cause the outage of a telephony network, which could in turn affect the continuity (or availability) of emergency call centres. The continuity requirements for emergency call centres are high and therefore also the continuity requirements for the telephony service and the datacentre of the provider are high.

[14] *There is some overlap between the two types: Cyber attacks can cause cyber disruptions (for example in DDoS attacks the goal is to create an outage).*

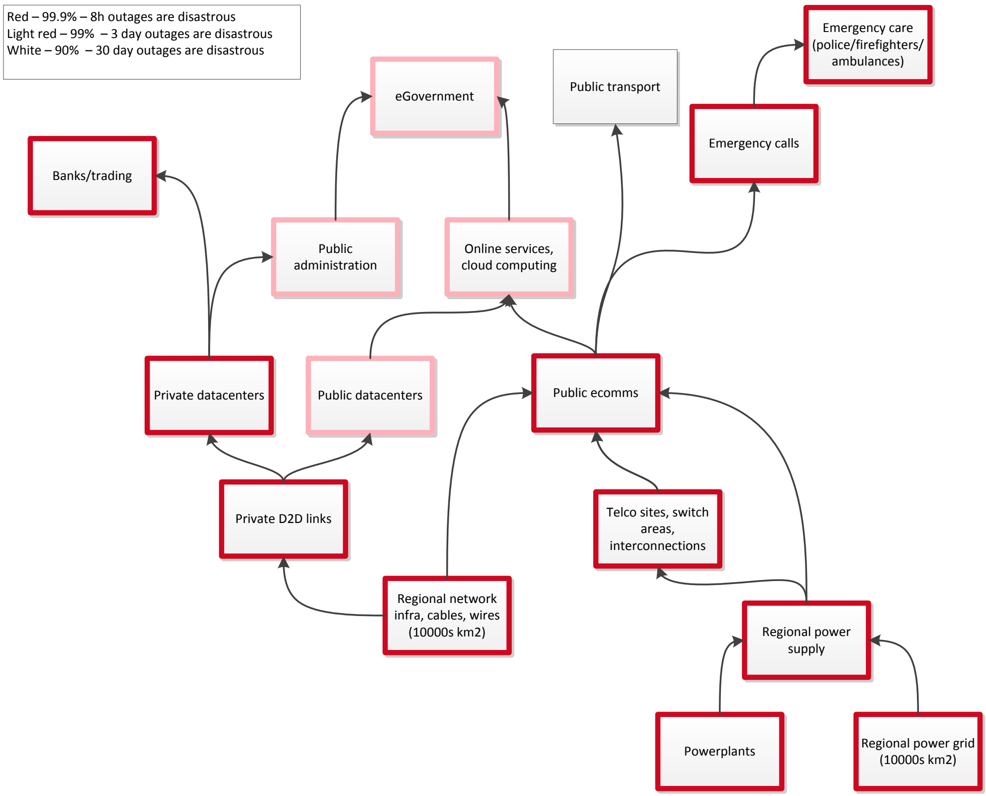
Red – 99.9% – 8h outages are disastrous
Light red – 99% – 3 day outages are disastrous
White – 90% – 30 day outages are disastrous
Emergency care (police/firefighters/ ambulances)
eGovernment
Public transport
Emergency calls
Banks/trading
Public administration
Online services, cloud computing
Private datacenters
Public datacenters
Public ecomms
Private D2D links
Telco sites, switch areas, interconnections
Regional network infra, cables, wires (10000s km2)
Regional power supply
Powerplants
Regional power grid (10000s km2)

Figure 2 Dependencies on the continuity of services and the integrity of infrastructure

Public sources on cloud computing outages show that the number of users affected per outage is increasing. Recent outages already affect in the order of millions of end-users.

- Gartner analysed the highly publicised services outages during the last 10 years, and came to the conclusion that the number of cloud service outages (48 cases) outnumbered the more traditional datacentre outages (29 cases), and that 47% of all documented large outages were caused by cloud services outages[15], with a visible acceleration in the past two years (12 cases in 2010 and 10 in 2011). The duration of cloud outages ranged between 40 minutes and five days with an average of 17 hours.
- Ponemon Institute studied the financial impact of downtime at datacentres by looking at 41 independent datacentres in the United States[16] and found that outages on average cost 500,000 US$ (ranging from 40,000 US$ up to a 1 million US$) and that costs are proportional

[15] Gartner, "The Realities of Cloud Services Downtime: What You Must Know and Do", 20 October 2011

[16] http://blog.newvem.com/main/2011/08/availability-story-of-the-inevitable-outage-of-the-cloud.html

to the duration of the outage, and the size of the datacentre. On an average a data centre downtime cost about US$5,600 per minute.

This should not come as a surprise. Consolidation (of services and infrastructure) means that the impact of a failure is also bigger. It is difficult to tell if the overall impact of outages and breaches is decreasing (or increasing) because of the adoption of cloud computing. Note also that while there is some data and press coverage about larger outages (affecting many end-users), but there is hardly any data about smaller incidents (regarding data breaches and outages). This makes it difficult to compare the impact of (presumably many, but smaller) incidents in legacy systems with the impact of outages concerning cloud services. Cyber attacks

In some settings it is also important to take into account logical dependencies between critical services, for example via software or secret information like passwords.

For example, consider an attacker who manages to alter software or access secret data at an IT vendor which delivers information technology to a range of organisations. The attack could have consequences across a range of organisations which use the software of this vendor. Recent examples include:

- the attack on RSA Secure ID, which had an impact on a range of (otherwise unrelated or disconnected) organisations using the RSA tokens.
- the attack on Diginotar which had an impact in Iran and across the Dutch e-government.
- the attack on Google, Adobe, Juniper, et cetera, called Aurora, which saw cyber attackers target source code repositories

We illustrate this type of dependency in Figure 3 where we take as an example an IT vendor who delivers office software to a range of organisations (banks, hospitals, power plants, and public office) who install the software locally on user machines. The security of these organisations depends on the security of the IT vendor and in particular the security of the service delivery processes (software development e.g.). An internet outage at the IT vendor would not have a direct impact, a cyber attack at the IT vendor, for example tampering of the source code by an attacker, could have a large impact.

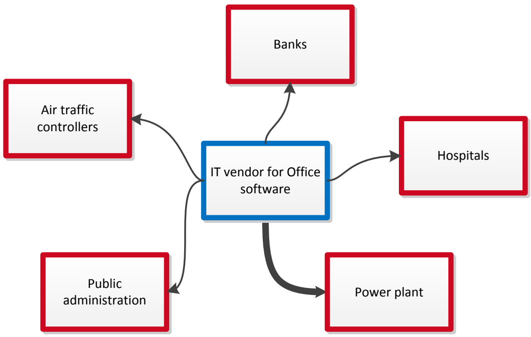

Figure 3. Logical dependencies on an software vendor

3.3 Relevant threats

From a CIIP perspective the relevant threats are different than the threats to consider from an SME perspective. Take for example one of the high risks in ENISA's 2009 cloud computing risk assessment for SMEs: vendor lockin. Vendor lockin is a high risk for an SME, and the associated costs (switching costs, or high bills) can be high. At the same time, a vendor lockin does not have a direct impact on the health, safety, security, or economic well-being of citizens. Similarly, although subpoena or e-discovery may be a relevant risk to take into account from an SME perspective, it is not relevant from a CIIP perspective, because access of law enforcement to certain data stored at the cloud computing provider does not have a direct impact on the economy or the society.

Based on the survey of past outages, we select the key threats which can have a large- scale impact:

For cyber disruption the most relevant threats are:

- Natural disaster, power outage, or hardware failure
- Resource exhaustion (due to an overload or a DDoS attack)
- Cyber attack (due to a software flaw)
- Administrative or legal issues

For cyber attacks the most relevant threats are:

- Resource exhaustion (due to a DDoS attack)
- Cyber attack (due to a software flaw)

In the next section we will look at several scenarios involving critical sectors, and we focus on these threats.

4 Cloud computing scenarios

We look at two types of large-scale security incidents: large disruptions (or outages) and cyber attacks, by discussing 4 different scenarios where cloud services are critical – in each scenario we look at different threats:

- Financial services
- Health services
- eGovernment services
- Cloud services

These scenarios are based on public data about usage of cloud computing services and past incidents.

We look at 4 different key threats to cloud computing services:

- Natural disaster, power outage, or hardware failure
- Resource exhaustion (due to an overload or a DDoS attack)
- Cyber attack (due to a software flaw)
- Administrative or legal issues

Note that we discuss a number of large security incidents (breaches and outages) related to cloud computing, to give an overview of relevant threats. We do not intend to make a comparison with security incidents in traditional IT deployments – and we do not want to suggest that cloud computing is more vulnerable than traditional IT.

For the sake of illustration we provide several examples, referring to public sources about cloud services, cloud customers, security incidents, and so on. By no means is it our intention to single out individual organizations for praise or criticism.

4.1 Financial services

We look at the scenario of a large financial services company using cloud computing. In the financial services sector a range of services are now being implemented using cloud computing.

- In 2011 Banco Bilbao started using cloud for email and calendar applications. The bank has 100.000 employees across the globe[17].

- In 2011 NYSE Euronext announced the creation of Capital Markets Community Platform, a community cloud for traders, offering on-demand computing resources.

- In 2012 the NASDAQ OMX Group announced the launch of FinQloud, a new cloud computing platform powered by Amazon Web Servicses and exclusively designed for the financial services industry.

Assume a trading platform, implemented using cloud computing technology. The set-up is as depicted in Figure 4.

- Full duplication of systems across multiple data centres.
- Private network links between datacentres are duplicated.

[17] http://www.pcworld.com/businesscenter/article/247851/spanish_bank_to_move_100000_employees_to_google_apps.html

- Inside datacentres, all systems are duplicated, planning for minimal downtime.
- The platform has a public (web-facing) interface for traders.

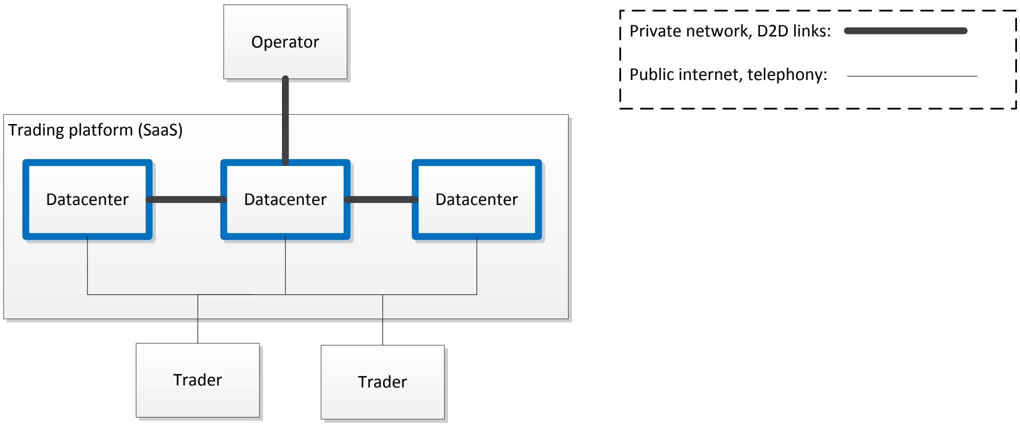

Figure 4. Trading platform implemented using cloud computing

4.1.1 Cyber attack

Suppose a cyber-attack was waged against the trading platform. Trading systems are generally considered part of a nation's critical information infrastructure.

- An attack of this kind took place at NASDAQ in 2010. In that case the attack did not impact trading. The attack was discovered only months later. NASDAQ sustains there was no direct impact on trading or assets.

Let's assume the computers of operators were infected with malicious software, which in turn exploits flaws in the trading platform, providing the attackers access to privileged financial data. The attackers obtain access to the control functions of the financial transaction system and they are able to tamper with trades causing large financial losses. A fault tree for this scenario would be as follows.

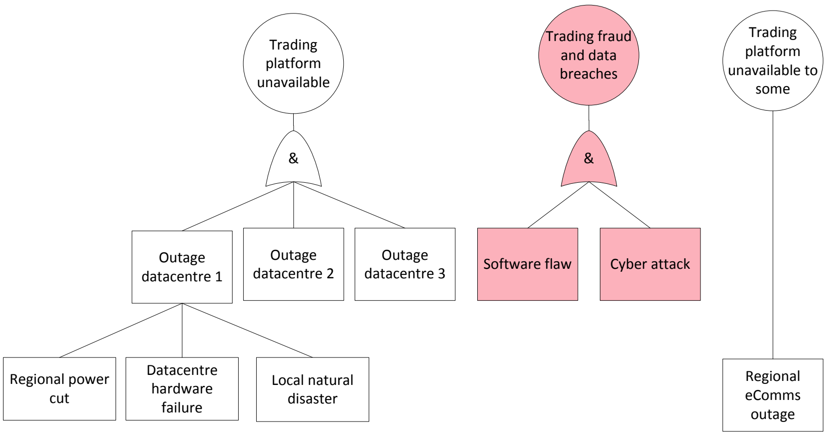

Figure 5. Impact of a cyber attack on a trading platform

Outages of the public network would prevent traders from reaching the trading platform, but regional outages only have only a limited impact, on some of the traders. All the faults affecting single datacentres are mitigated by the redundancy across the datacentres. This mitigates the impact of, for example, regional power cuts. Physical redundancy, however, does not help to prevent a cyber attack which exploits a flaw in the software of the trading platform.

4.1.2 Other cyber-attacks affecting cloud computing services

There are other examples of cyber attacks on cloud computing services with a large-scale impact:

- In 2012 Credit card processor Global Payments said there had been a security breach that exposed 1.5 million consumers to (credit card) fraud. The incident is costing Global Payments an estimate $84.4 million dollars.
- In 2012 LinkedIn was breached and 6.5 million unsalted SHA-1 hashed passwords were found on underground forums. Linkedin has 160 million members worldwide.
- In 2012 Zapos fell victim to a cyber attack which breached data of about 24 million customers, including customer names, email addresses, physical addresses, phone numbers, the last four digits of the customer card numbers and encrypted passwords.
- Epsilon was hacked in early December 2011, and leaked data included information relating to the customers of at least 50 companies, including Best Buy, Citi, Hilton, LL Bean, Marriott, Target, TiVo, and Walgreens.

Key points

The set-up of the trading platform is focussed on physical redundancy. The main goal is to prevent outages due to high loads or power cuts or incidents affecting individual datacentres. In such a setup the overall risk of disruptions decreases. At the same time cyber-attacks which exploit software flaws can cause very large data breaches, affecting millions of users directly.

- Security is crucial for critical cloud computing services – one flaw can impact a wide range of organizations directly. From a logical perspective the cloud computing service is a single point of failure.
- Cloud service providers have the scale and resources to address and prevent cyber attacks in a more professional way than most other organizations. It is important to prevent and mitigate the impact of cyber attacks by creating also logical redundancy – that is, to use different layers of defence and to use separate systems with a different logical structure, to cross-check transactions and to detect attacks.

4.2 Health services

A number of hospitals are now adopting cloud computing. Information technology and cloud computing in particular are expected to bring important efficiency gains. We give some examples:

- By 2011, about 30% of the healthcare organizations had developed a strategic plan for adopting cloud computing services[18]. It is expected that by 2016 about 30% of IT budget of healthcare organizations would be devoted for cloud computing based expenses. 73% plan to make greater use of cloud-based technologies in the future[19].
- In 2010, a leading Italian children's hospital switched to an online solution for email services for its 2500 employees[20]. Another Italian hospital USL of Asolo in Veneto is reported to be using cloud computing to help operative tasks[21].
- The Swedish Red Cross adopted a cloud computing solution to help them reduce their costs by about 20% and enhanced communication in real time between its employees[21].
- A Russian cardiovascular centre, Penza, adopted a cloud computing solution to coordinate activities, diagnosis and decisions on treatment and surgery between doctors around the country, with crucial gains for the patients[22].

Consider a scenario where the data centre is set up with:

- Redundant power and cooling - two independent power grid feeds are taken into an uninterruptible power supply (UPS) system that powers ICT and cooling systems
- UPS has dual feeds to all equipment within the data centre.
- Diesel generators rated to carry the entire data centre load.

In the event of grid loss, the UPS maintains electrical load until the generator has started and spun up to load, and the generator is fuelled with enough diesel to maintain supply for a day. Such facilities will contract with a fuel supplier to start tanker refuelling of the generator immediately upon loss of mains power (with the understanding that the logistics of supply are such that it could take up to 24 hours to replenish the local fuel tank).

We assume that the datacentre is one of several other datacentres providing the cloud service to users, as depicted in the diagram below:

[18] From Tactic to Strategy: The CDW 2011 Cloud Computing Tracking Poll, 2011 http://webobjects.cdw.com/webobjects/media/pdf/Newsroom/CDW-Cloud-Tracking-Poll-Report-0511.pdf

[19] Six questions every health industry executive should ask about cloud computing, Accenture, 2010

[20] "Economics of Cloud Computing" http://www.intertic.org/Policy%20Papers/Report.pdf

[21] "Understanding Cloud Computing Competition, Environment and Finance" http://www.intertic.org/Policy%20Papers/EBR.pdf

[22] Understanding Cloud Computing Competition, Environment and Finance, European Business Review, 2011

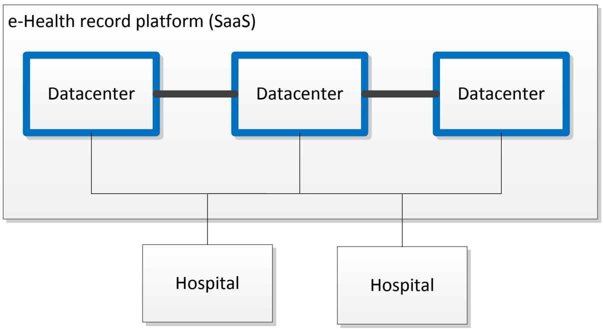

Figure 6. e-Health record platform using cloud computing

4.2.1 Natural disaster

Consider a severe weather event which impacts the regional power supply and the data centre. For example, high volumes of precipitation during summer storms in the UK, have caused flash flooding in areas not normally deemed to be high-risk flood risk areas. Data centres are often located in rural areas, outside of conurbations, and as such are highly dependent on the surrounding infrastructure (power, communications, drainage and transportation) in order to maintain services.

Most datacentres are equipped with redundant power grid connections and backup generators to mitigate the impact of extreme weather and power cuts. When a power cuts persists, of course, resupply of generator fuel becomes an issue. In Japan, following the earthquake, in fact there are now discussions to prioritize fuel for datacenters[23].

- **(2 hours, millions of users)** In June 2012 a severe thunder storm affected an Amazon EC2 datacenter. The outage caused problems for some major websites with millions of users, like Instagram, Netflix and Pinterest.
- **(48 hours, large segment of multiple clouds)** In August 2011, a lightning strike in Dublin caused Microsoft BPOS, the Amazon EC2, and its Relational Database Service (RDS) to be out for several hours[24]. It took over 48 hours for full functionality to be restored on the AWS service.

[23] https://www.datacenterknowledge.com/archives/2011/03/15/japan-may-prioritize-power-for-data-centers/

[24] http://www.datacenterknowledge.com/archives/2011/08/07/lightning-in-dublin-knocks-amazon-microsoft-data-centers-offline/

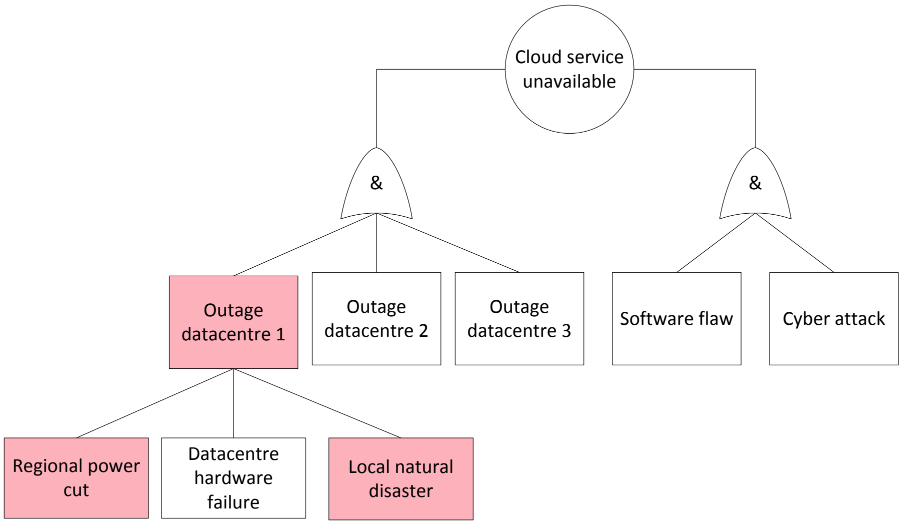

Figure 7. Impact of natural disaster

Let's assume bad weather (heavy rain) causes a regional power cut and that the fuel supply fails to arrive at the datacentre, due to the flooding, and that the datacentre eventually goes offline. In a redundant cloud computing setup an outage at a single datacentre has limited impact on the continuity of services. In this case the availability of e-health records, for example, would be guaranteed, because the other datacentres can take over the load.

Key points

A key benefit of cloud computing is resilience to withstand regional power cuts or local natural disasters. It is difficult to mitigate the impact of fairly common events like floods, storms, or earthquakes in a set up with only a single datacentre.

- Cloud computing services can be more resilient, and the risk of disruptions due to natural disasters decreases.

4.3 eGovernment services

A number of public sector organisations are now using IaaS, PaaS and SaaS services, to implement internal IT and to implement e-government services, in a more efficient way .

- The UK G-Cloud "framework", worth up to £60 million will operate for an initial six-month period, after which successful applicants will be able to sell a range of tools the government expects will include email, word processing, hosting, ERP, records management, CRM and other office productivity software[25].

[25] http://www.itnews.com.au/News/282746,sme-suppliers-rush-on-uks-g-cloud.aspx

- The UK Gov Cloud app store "GovStore"[26] has over 1,700 information and communications services available to the UK public sector, and contains details of each of the suppliers and their services.
- In 2011, the Catalan Government, the largest user of cloud computing public services in Spain, had over 741,000 business users and organisations (such as Ferrovial, MRW, Government of Aragon, and Madrid City Council) take advantage of the technology[27].

We assume that the datacentre is part of a number of datacentres supporting the provisioning of a SaaS cloud platform, specifically for government organizations. In this way several government organizations can set-up (in a scalable, and quick fashion) e-government services to serve the citizens. The set-up is depicted in Figure 8. The datacentres have the scale to deal with peak loads on either of the websites.

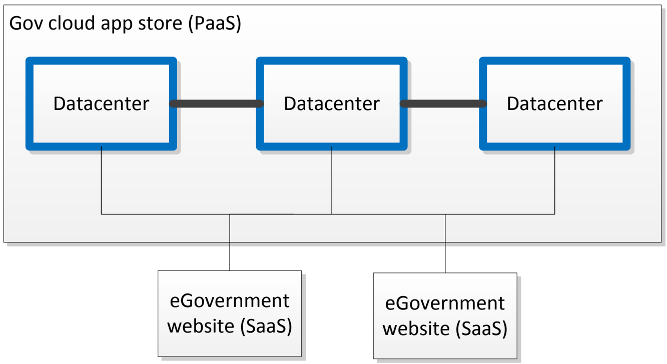
Gov cloud app store (PaaS)
Datacenter
Datacenter
Datacenter
eGovernment website (SaaS)
eGovernment website (SaaS)

Figure 8. A gov-cloud appstore used for eGovernment web services

4.3.1 Overload

Consider the situation of a big disaster and a rush for information on one of the (e-Government) websites for public disaster information. For example, in 2012, following a large explosion, a local Dutch radio station referred citizens to an emergency webpage, for emergency information. The website went offline immediately due to an overload of visitors.

The elasticity of cloud computing prevents an outage because the service runs on some very large datacentres with vast computing power. Large peak loads of the e-Government websites have been taken into account.

[26] http://www.govstore.net/

[27] http://catalannewsagency.com/news/society-science/microsoft-chooses-catalan-government-promote-%E2%80%98cloud-computing%E2%80%99-europe

Key points

Cloud computing makes it easier to mitigate a surge in traffic, due to a particular event or a deliberate (DDoS) attack, and in this way prevent an outage. It would be prohibitively expensive to implement a datacentre with the required scale to handle such peak loads.

4.4 Software as a cloud service

A number of cloud service providers, who offer so-called Software as a Service (SaaS) to customers, rely on other cloud service providers to provide more basic IT resources, such as operating systems and application servers (called IaaS or SaaS providers).

- **Amazon 2011:** Amazon infrastructure is reported to carry as much as 1% of the all internet consumer traffic in North America and on an average a third of all internet users visit an AWS powered site daily[28]. Amazon reports having customers like Zynga, Reddit, MySpace, Netflix, Dropbox, HootSuite, et cetera.

Consider the following setup where two different IT vendors rely on the same underlying IaaS/PaaS provider for basic IT resources.

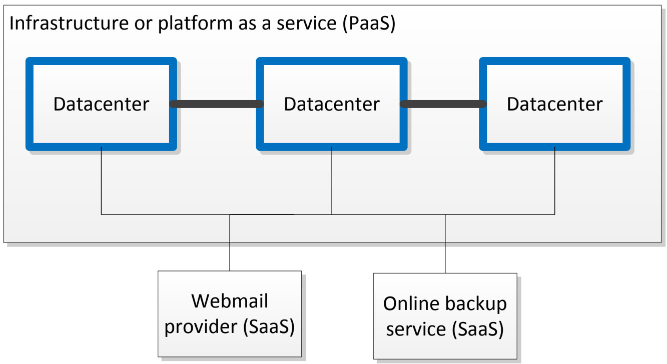
Infrastructure or platform as a service (PaaS)
Datacenter
Datacenter
Datacenter
Webmail provider (SaaS)
Online backup service (SaaS)

Figure 9. e-Government applications (SaaS) running on a governmental app store (PaaS)

4.4.1 System failure

Let’s assume the IaaS/PaaS provider suffers an outage due to a system failure, say a software flaw. There are numerous examples of cases where flaws and failures affect the services of IaaS/PaaS providers:

- **(24 hours, multiple regions)** Microsoft Azure was offline from 28th February 2012 due to a leap year problem. The outage affected the compute service in a number of regions[29]. Service

[28] http://blog.deepfield.net/2012/04/18/how-big-is-amazons-cloud/

[29] https://blogs.msdn.com/b/windowsazure/archive/2012/03/01/windows-azure-service-disruption-update.aspx

to majority of customers was restored in around 9 hours, while full service restoration took another 24 hours[30]. The affected customer base included the UK G-Gov CloudStore[31].

- **(48 hours, large segment of users)** In April 2011 Amazon's EC2 cloud suffered multiday outages resulting in loss of availability and loss of data. This took down the data of several high profiles sites including Reddit (over 36 hours[32]), Foursquares, Hootsuite and Quora (48 hours[33]).
- **(10 hours, service-wide)** VMWare Cloud Foundry suffered two outages in April 2011 due to power outage (10 hours) and subsequent misconfiguration (90 minutes)[34].
- **(3 hours, service-wide)** Microsoft BPOS suffered various outages in May 2011 due to three different issues, creating lengthy email backlogs that created delays of upto 3 hours[35].

The impact of failure at an IaaS/PaaS provider can have an impact across a range of organizations, affecting many end-users. It can also have strange side-effects. Take for example an organization which relies on the webmail provider for emails and on the online backup provider for backups, to mitigate outages or data loss at the webmail provider. In case of a software flaw the organization would still risk its vital data because both services rely on the same underlying IaaS/PaaS provider.

4.4.2 Other system failures causing large outages or data loss

System failures causing outages are not rare. Below we list a number of examples of incidents in which a system failure caused a large-scale outage or data loss.

- **(24 hours, 7,500 users)** In March 2009 7,500 Carbonite customers lost their backups. Eventually after over 24 hour, all except 54 of these customers were able to retrieve their backups[36].
- **(Two months, 1 million users)** In October 2009 T-Mobile's Sidekick 1 million users lost their contacts, calendar entries, to-do lists and photos when Microsoft subsidiary Danger suffered a server failure[37].

[30] https://blogs.msdn.com/b/windowsazure/archive/2012/03/01/window-azure-service-disruption-resolved.aspx

[31] http://www.guardian.co.uk/government-computing-network/2012/feb/29/cloudstore-gcloud-microsoft-azure-outage

[32] http://www.reddit.com/r/announcements/comments/gva4t/on_reddits_outage/

[33] http://www.quora.com/Why-is-some-data-missing-from-Quora-after-the-April-2011-outage

[34] http://www.networkworld.com/news/2011/050211-vmware-foundry-outage.html

[35] https://blogs.technet.com/b/msonline/archive/2011/05/13/update-on-bpos-standard-email-issues.aspx

[36] http://techcrunch.com/2009/03/23/online-backup-company-carbonite-loses-customers-data-blames-and-sues-suppliers/

[37] http://techcrunch.com/2009/10/10/t-mobile-sidekick-disaster-microsofts-servers-crashed-and-they-dont-have-a-backup/

- **(Permanent data loss, over 6300 users)** Between 1-4th July 2010, Evernote experienced several hardware failures leading to loss of data of over 6,323[38] Evernote customers.
- **(48 hours, service-wide)** In December 2010 17,355 Microsoft Hotmail accounts lost all emails for two days before it was restored by the provider[39].
- **(Four days, 35,000 users)** In February 2011 over 35,000 Gmail accounts and Google Apps customers lost all the data in the accounts. Google had to resort to restoring backups from tapes, in an operation lasting four days[40].
- **(Several hours, service-wide)** On 6,11 and 15 August 2008, Google's enterprise e-mail system, Apps Premier Edition, suffered an outage and disrupted some organizations and users that rely on the service[41]. One of the outages affected nearly all users for approximately two hours; while the other two affected part of the user base for about 24 hours.
- **(30 minutes, service-wide)** In September 2011, Google Docs, Google Docs List and Google went offline for a period of around 30 minutes, affecting all its users[42].
- **(72 hours, as big as 70m users)** Millions of Blackberry users across Europe, Middle East and Africa suffered outage for three days in October 2011. The company has about 70m users around the world. Speculation is that most of the global customer base may have been affected at some point during the 72 hours[43].
- **(Seven hours, 3.8 percent of customer base)** In February 2012 Microsoft Azure platform suffers outage that lasted more than seven hours, affecting 3.8% of the customer base[44].

Key points

It is quite common for (SaaS) cloud computing providers to rely on other (IaaS/PaaS) cloud computing providers. These relations create more dependencies between organizations and between cloud computing service providers. Outages or other incidents at a single service provider could have an impact on a range of organizations, including other cloud service providers and customers.

- Cloud computing services are not immune to system failures – overall the risk of system failures may be reduced when compared to traditional IT deployments, but if a system failure occurs then there may be a large impact (and a lot of media attention).
- Particularly for IaaS and PaaS providers it is crucial to mitigate outages and system failures because so many other cloud service providers or other organizations depend on them.

[38] http://blog.evernote.com/2010/08/09/july1/

[39] http://www.theregister.co.uk/2011/01/04/microsoft_apologizes_empty_hotmail/

[40] http://blogs.computerworld.com/17897/google_apps_and_gmail_outage_outrage_problem_resolved

[41] https://www.gartner.com/DisplayDocument?ref=seo&id=750739

[42] http://www.informationweek.com/news/cloud-computing/software/231600978

[43] http://www.huffingtonpost.com/2011/10/13/blackberry-outage-2011-rim-says-services-returning_n_1008596.html

[44] http://www.theregister.co.uk/2012/02/29/windows_azure_outage/

4.5 Administrative or legal disputes

Another type of outage which is worth mentioning are outages caused by administrative or legal disputes. We give a number of examples:

- **(Permanent data loss, service-wide)** The Megaupload cloud storage service was taken down by the US prosecutors alleging copyright infringement. At the time of closure it had 180,000,000 registered users hosting over 25 petabyte (25000 terabyte) of storage[45]. It was the 13th most visited site on the Internet.
- **(Permanent shutdown, 20,000 users)** In August 2008, The Linkup, a service offering online data storage lost access to unspecified amount of customer data and soon after on 8th August shutdown the service, effecting over 20,000 paying customers[46].
- **(Permanent shutdown, unknown number of users[47])** In February 2009, Onsite3, a leading global provider of electronic evidence solutions for law firms and corporations filed for Chapter 11 bankruptcy and that it is being bought over by Integreon, a provider of outsourced knowledge, legal, and administrative support services[48].

We do not go into details about this kind of threat much further, because technically this threat is not specific for cloud computing, but could affect any kind of ICT service provider. At the same time we would like to stress that the criticality of certain cloud computing services raises the issue of such administrative or legal disputes. If a very large cloud computing service provider stops services over a legal dispute then a large number of customers is affected, and the impact on the economy and on society can be significant.

Key points

Administrative and legal issues concerning a cloud computing provider are amplified by the sheer size of cloud computing services.

- Cloud computing services are not immune to administrative or legal issues. If there is a legal dispute involving the provider or one of its customers, then this could have an impact on the data of all the other co- customers (or co-tenants).

[45] http://en.wikipedia.org/wiki/Megaupload

[46] https://www.networkworld.com/news/2008/081108-linkup-failure.html

[47] Indicative customer base number not available

[48] http://www.bizjournals.com/washington/stories/2009/02/02/daily105.html?page=all

5 Conclusions & Recommendations

In this paper we have looked at cloud computing from a CIIP perspective. We gave an overview of public sources on cloud computing uptake and we look at different cloud computing scenarios large cyber attacks and large cyber disruptions.

Conclusions

We summarize our conclusions:

- **Cloud computing is critical:** Cloud computing usage is growing and in the near future the vast majority of organizations will rely on some form of cloud computing services. This makes cloud computing services critical in themselves. Cloud computing is being adopted also in critical sectors, like finance, energy and transport.
- **Cloud computing and natural disasters:** A key benefit of cloud computing is resilience in the face of regional power cuts or local natural disasters. It is difficult to mitigate the impact of fairly common regional disasters like floods, storms, or earthquakes in a set up with only a single datacentre, or a traditional set-up with a legacy onsite IT deployment.
- **Cloud computing and overloads or DDoS attacks:** Elasticity is a key benefit of cloud computing and this elasticity helps to cope with load and mitigates the risk of overload or DDoS attacks. It is difficult to mitigate the impact of peak usage or a DDoS attack with limited computing resources.
- **Cyber attacks:** Cyber attacks which exploit software flaws can cause very large data breaches, affecting millions of users directly. The impact of cyber attacks is multiplied by the concentration of resources which is a result of the uptake in cloud computing.
- **IaaS and Paas the most critical:** The most critical services are large IaaS and PaaS services which deliver services to other IT vendors who service in turn millions of users and organisations.
- **Administrative and legal disputes:** Cloud computing is not immune to administrative or legal issues. If there is a legal dispute involving the provider or one of its customers, than this could have an impact on the data of all the other co- customers (or co-tenants).

Recommendations

The CIIP action plan calls for a discussion on a governance strategy for cloud computing. Below we make several recommendations for policy makers and national CIO's that should be taken into account when setting such a strategy. From a CIIP perspective the goal would be to prevent large security incidents. Governance of security, across a region, a sector, or group of providers, can be subdivided in three key processes (see figure 10):

1. RA: Making a risk assessment – to determine which are critical infrastructures, what is their value for economy and society, and what kind of incidents need to be prevented.
2. SM: Taking security measures (or make sure they are taken) – to prevent large incidents or to mitigate their impact.
3. IR: Collecting incident reports – to understand weaknesses in security measures and to evaluate and validate the risk assessment.

This triangle of governance processes can be supervised by a government authority (a regulator, say) or some industry association (a body of auditors, say), or in combination. We make several recommendations for each of these processes.

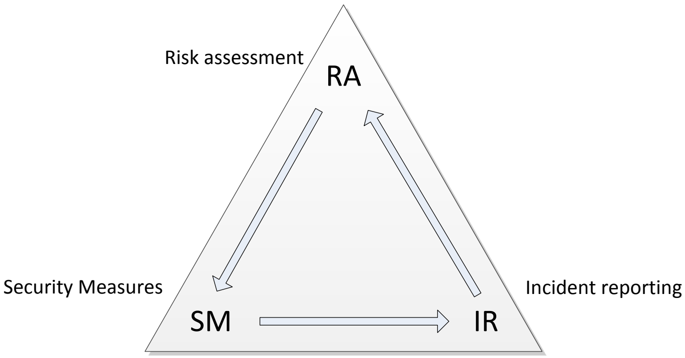

Figure 10. Key security governance processes

5.1.1 Risk assessment

Risk assessment is at the start of governance. The main goal of risks assessment is to prioritize security measures. We make several recommendations related to risk assessment.

- **Assets in scope:** It is important to take a pragmatic approach and address the most critical cloud computing services first. It is easy to say that 'all cloud computing services are critical' but it is infeasible to address all cloud computing services at once. As mentioned, since outages at IaaS or PaaS providers can have an impact across a range of organizations, this means that these services should be treated with priority. Often in cloud computing a range of SaaS services depend on a IaaS/PaaS services and network connections and power supply. The IaaS/PaaS service depends on network connection and power supply. This suggests that the criticality of power supply and network connections is higher than the criticality of the IaaS/PaaS provider, and that the criticality of the IaaS/PaaS provider is higher than the SaaS provider.
- **Assessing dependencies on cloud computing:** Most countries, when making national risk assessments, from a critical infrastructure perspective, take into account already power supply and electronic communications networks. They should also take into account large cloud computing services and large datacentres. Agencies responsible for establishing and maintaining national contingency plans should take into account the dependencies of modern society on IT.
- **Transparency about logical and physical dependencies**: A risk assessment requires a clear view of the dependencies. It should be clear which critical operators and critical services depend on which cloud computing services. The special nature of cloud computing plays a role here. It is inherent to the cloud computing model, that hardware and software is shared between multiple tenants. This is exactly what creates a benefit when it comes to withstanding DDoS attacks or peak loads. At the same time, this complexity in dependencies can create strange side-effects. Outages at an underlying IaaS or PaaS provider can affect a range of (otherwise unrelated) services across society. It is important to map the main logical and physical dependencies.

5.1.2 Security measures

The main goal of security governance is to mitigate incidents by taking security measures.

- **Foster exchange of best practices to achieve a security baseline:** It goes without saying that it is important that cloud providers take appropriate security measures. There is a host of literature on best practices, ranging from best practices on how to set-up datacentres and networks, to how to securely engineer software and services. In this document we refrain from making specific technical recommendations about these best practices, so for example, we do not go into details about best practices like 'deploying security patches to operating systems'. We do stress that it is important for government authorities to support and foster the exchange of such best practices. Security is constantly changing and security measures must be improved continuously. Government authorities should encourage an open culture of exchange and discussion about security measures. Security is about continuous improvement and government authorities should avoid a situation where a specific set of best practices is cast in stone (by regulation or self-regulation).
- **Logical redundancy:** We would like to stress one particular issue: Cloud computing services are often set-up with several redundant datacentres to withstand outages of single datacentres (due to power cuts or natural disasters, for example). However, most cyber attacks capitalise and exploit software flaws, which are persist across the datacentres. Software flaws can cause outages by themselves. Arguably, cloud service providers have the scale and resources to address and prevent software flaws and cyber attacks in a much more professional way than most other organizations. Still it is important to of the concentration important to prevent and mitigate the impact of cyber attacks by creating also logical redundancy – that is, to use different layers of defence and to use separate systems with a different logical structure, to cross-check transactions and to detect attacks.

- **Physical redundancy:** Related to the previous point, most relevant threats, from a CIIP perspective, are related to lack of logical or physical redundancy. A single point of failure must be avoided. One effective way to do this is to make sure that the software and hardware are standardized and not dependent on specific technology of a specific provider. Standardization, especially for IaaS and PaaS services, would allow customers to move workload to other providers in case one provider has an issue. If a service is standardized and if frequent backups are made, then even an outage caused by an administrative or legal dispute can be addressed, by simply taking the backups and deploying them at the site of another (competing) cloud computing provider. This kind of mutual aid is only possible when the cloud services infrastructure is standardized. From a CIIP perspective standardization in cloud computing is very important, because it allows customers to mitigate any (legal or administrative) issues they may have with the cloud service provider.

- **Audits, tests, and exercises:** There is a lot of information security literature about the importance of auditing and testing systems. Cloud computing providers should schedule frequent audits and tests, by internal testers and auditors, and, when relevant, by external testers and auditors. In discussions about governance, often the need for independent external auditors is stressed. Such audits are often organized as part of a certification process. We would like to stress that ICT systems are constantly changing (software is updated daily) and that this reduces the effect of periodic (yearly) audits. Moreover, the complexity of the systems underpinning cloud computing services makes it very difficult to assess security or resilience. Cloud computing providers and government authorities should ensure there is a continuous program of audits, tests and exercises in place. Audits by external parties are only one part of this program.

5.1.3 Incident reporting

Incident reporting provides the cross check on the effectiveness of security measures and it provides input to the risk assessment.

- **Mandatory reporting:** Without incident reports it is very difficult to understand the impact of security incidents on cloud computing providers. This complicates risk assessment, both for cloud computing service providers, as well as, at a national level, for government authorities like contingency agencies. Lack of data about incidents makes it very difficult to prioritize security measures, and in this way security governance becomes inefficient or even ineffective. Government authorities and cloud providers should agree on the thresholds for reporting and the type of services that should be in scope.
- **Legal consequences:** Secondly, it is important to consider the following. Certain cyber attacks are stealthy and their traces may be difficult to spot even for system administrators who know the cloud computing systems inside out. There is always a risk that security incidents are not reported to higher management or to authorities for fear of reprisal or legal consequences. Member States should consider the possible benefits of providing immunity for providers who reported security breaches which would otherwise go unnoticed.
- **Outages and security breaches:** While there are some good information sources about data breaches[49] there are no good information sources about cloud computing service outages. Reliable information is often difficult to find. And even for some fairly high-profile incidents it is difficult to find basic information like numbers of users affected or duration. To be able to assess overall risks and assess the effectiveness of security measures in place, it is crucial to have incident reports about outages and security breaches from a wide range of cloud computing providers.

[49] For instance http://datalossdb.org collects, and provides an overview of, data breaches.

6 References

Related ENISA papers

- The 2009 ENISA Cloud computing risk assessment assess risks and benefits for SMEs who consider adopting cloud computing.
- The 2011 ENISA report on security and resilience of Governmental clouds provides guidance for government organisations for selecting cloud computing services.
- The 2012 ENISA report on secure procurement of cloud computing services, focusses on monitoring service levels of cloud computing services.

Legislation

- The European Commission issued a European strategy for cloud computing.
- The European Commission communications on CIIP outline a number of priorities in the area of CIIP.

  The European Commission is preparing a cyber security strategy, addressing cyber security in critical sectors.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu