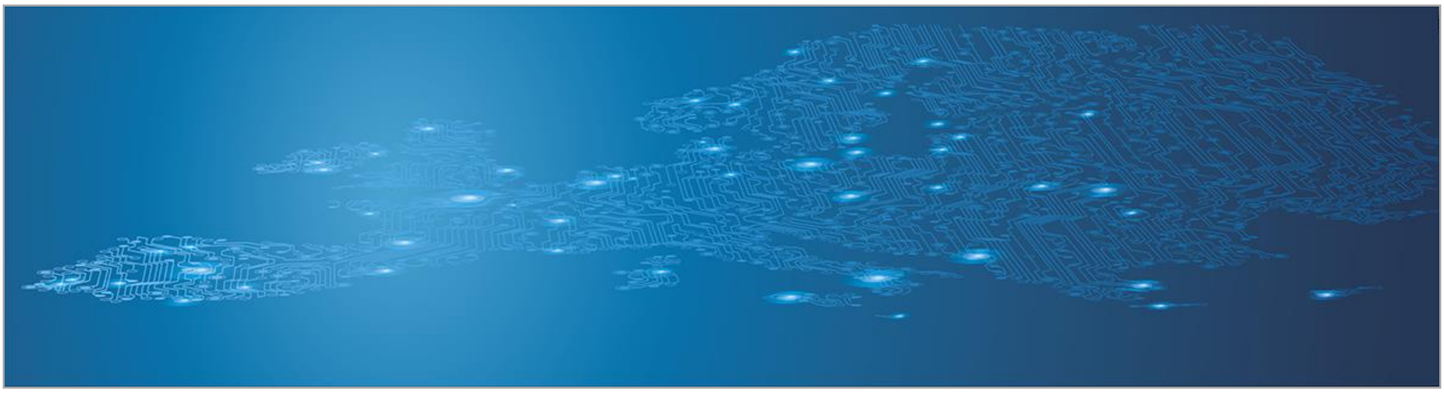


Incident handling in the cloud

Handbook, Document for teachers

September 2014

European Union Agency for Network and Information Security   www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (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.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

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

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 Regulation (EU) No 526/2013. 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.

Copyright Notice

Table of Contents

1 Introduction

Goal

In this exercise you will investigate methods to address cloud-based security vulnerabilities through a scenario where data is not always fixed to one physical server or location.

Target audience

This exercise is useful for incident responders of all experience levels.

Course Duration

5 hours

Frequency

Once per team

Structure of this document

	Task	Duration
	Introduction to cloud computing	60 min
	Cloud services overview	45 min
	Task 1: Exploits against a Cloud Infrastructure	90 min
	Incident 2: Cloud data: flexibility and control?	45 min

2 General Description

The growing prominence of cloud computing presents some new security challenges, some which are ‘back to the future’ and some that are more common to any computing environment. But what is this ‘cloud’ thing anyway and why does it seem to dominate IT journalism?

2.1.1 What is cloud computing?

2.1.1.1 Virtualised, dynamically allocated computing resources (processing, storage, even network infrastructure like firewalls and switches)

Definitions of cloud computing vary; however, one of the most commonly utilized definitions is from the U.S. National Institutes for Standards and Technology (NIST), which defines five ‘essential’ characteristics of cloud computing solutions, including on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.[1]

Cloud computing uses the above-mentioned virtualised resources, combined with shared storage and high speed network links to provide affordable, high-quality service. Customers of cloud service providers can store and process data in the cloud, manually or dynamically changing the number of instances in a particular processing job as needed. Customers may also choose to access applications hosted in the cloud – like Google's Gmail email application or Salesforce.com's Customer Relationship Management software.

2.1.1.2 Cloud service models

The simple distinctions between software, platform, and infrastructure-as-a-service models were listed by Jeff Caruso in Network World on 2 November 2011.[2]

- Software as a Service (SaaS) is a web-based service that takes the place of locally installed software applications, such as Gmail for email, document creation like Google Docs, or online customer relationship management systems.
- Platform as a Service (PaaS) provides a network-based framework for application development, like Microsoft Azure.
- Infrastructure as a Service (IaaS) provides storage or computational resources over a network, such as Amazon's Elastic Compute Cloud or Google's Compute Engine. Examples of storage-specific cloud vendors include Amazon Simple Storage Service, Google Cloud Storage, Microsoft Windows Azure Storage, Rackspace, Amplidata, cloud.bg and VPS.net

A more technical illustration of the distinctions between these three cloud service models follows below. This figure also shows which party – the provider and the client-tenant – provides what in a cloud service model. Additionally, from that service model the lever of responsibility could be deduced in the case of attack or any kind of service disruption. Note that in the Software as a Service model,

[1] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[2] https://www.networkworld.com/news/2011/102511-tech-argument-iaas-paas-saas-252357.html?page=1

the provider can provide the interface as well as in the case of Google's Gmail or hosted Customer Relations Management systems like Salesforce or SAP's Business ByDesign platform.

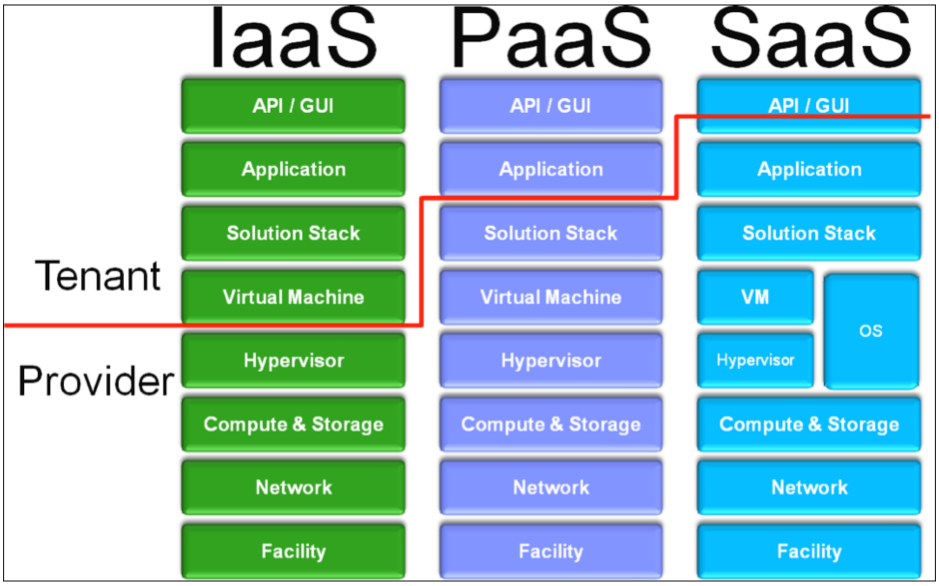


Figure 1: The delineation of responsibility within each of the cloud service models [3]

2.1.1.3 ENISA ProSecure Secure

ENISA offers the following document to describe various service level agreements in cloud computing contracts as well as ways in which cloud vendors handle incidents and attacks like DDoS and data centre outages. The document also examines cloud client or cloud vendor responsibilities in the SaaS, PaaS, and IaaS models.[4]

2.1.2 Why use cloud computing?

2.1.2.1 Common questions asked when deciding if one should move towards cloud solutions

Those boxes in my server room have served me well, why move the data somewhere out of my reach?

I've already virtualised as many servers as I can in my environment. What more can entrusting them to a third party vendor do?

2.1.2.2 Advantages of the cloud

Cloud vendors like Amazon and Google have far more resources in geographically diverse locations compared with most companies. This allows for greater fault tolerance for local issues like prolonged electrical outages or natural disasters.

Cloud vendors have expertise in keeping a widely distributed computing system running, freeing an organisation's IT staff to improve efficiency and to innovate rather than merely maintaining IT infrastructure. This shift of responsibility can include fundamental services like email and backup when

[3] http://pen-testing.sans.org/blog/2012/07/05/pen-testing-in-the-cloud

[4] *ENISA ProSecure Secure https://www.enisa.europa.eu/activities/application-security/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts*

an organisation moves from a local Microsoft Exchange server to cloud-based email service, where backup is being outsourced and the need for physical server in the company premises has been diminished.

Cloud companies usually offer scalability. In a virtual environment like VMware, a system administrator can dynamically increase or decrease the amount of memory, storage space, processor speed, and network bandwidth given to virtual machines. Yet, in the end, the VMware host system only has so much total memory, storage, and processing power to allocate. A cloud environment can scale up to spread the load to many systems in multiple datacentres.

Depending on the cloud vendor's service model and contract, scaling up or down in any resource may happen automatically or at a customer's request and this change can last only as long as a customer needs. This presents quite a shift from needing to plan out a server's capacity not just for an immediate project but going forward for several years. Traditionally, IT staff must configure and then maintain that server as it ages and becomes less reliable. In the cloud, you pay only for what you need now and you can easily get more when you need more in the future.

2.1.3 Who uses cloud computing?

Google and Amazon, for example, each claim millions of business, education, government, and non-profit customers from large corporations like Konica Minolta, Fairchild Semiconductor and Land Rover to small neighbourhood associations and charities as their customers.

2.1.4 ENISA Video

Project the video at the following URL for all trainees to review ENISA's recommendations about cloud computing risk assessment: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing

After the video, allow the class to have a break for 15 minutes.

2.1.5 Plenary discussion (0–20 minutes, depending on trainees' prior experience with the cloud)

As in many newer areas of technology, we can learn much by sharing our own experiences with using and migrating to (and from) the cloud. Ask the class 'Has any one created, used or moved a service to a cloud environment?' Ask those who can answer to share their experience, especially in terms of the following.

- What was the process?
- Were there problems?
- What were the benefits?
- How would you approach the project differently in retrospect?

2.1.6 Overview of how to use the cloud

Users access cloud computing using networked client devices, such as desktop computers, laptops, tablets and smartphones. Many cloud applications do not require specific software on the client and instead use a web browser to interact with the cloud application. Some cloud applications, however, support specific client software dedicated to these applications (e.g. virtual desktop clients and most email clients). Some legacy applications (line of business applications that until now have been prevalent in thin-client Windows computing) are delivered via a screen-sharing technology.[5]

[5] http://en.wikipedia.org/wiki/Cloud_computing

The sign up and configuration process to access a cloud resource varies by vendor and by service. A few examples follow. (These examples are in no way given as a recommendation to use these services.)

2.1.6.1 Presenting Google Apps for Business (Gmail migration) as an example

Registering a Google Apps for Business account, including private registration for a new domain name, obtaining email and web services and registering for cloud computing and storage, takes a few minutes. (The trainer should project this page on the whiteboard https://www.google.com/enterprise/apps/business/.)

Google's Service Level Agreement specifies an uptime of 99.9% with all disaster recovery and backup handled by Google. Employees are allowed to access HTTPS-encrypted email from anywhere in the world, can share information through ad hoc websites and access many other Google-related services and web-based applications, including Customer Relationship Management and other database tools. Google also provides bulk upload tools from existing email servers and a synchronization tool, keeping corporate standard email readers like Thunderbird or Outlook in use but with Gmail service as the back end server.

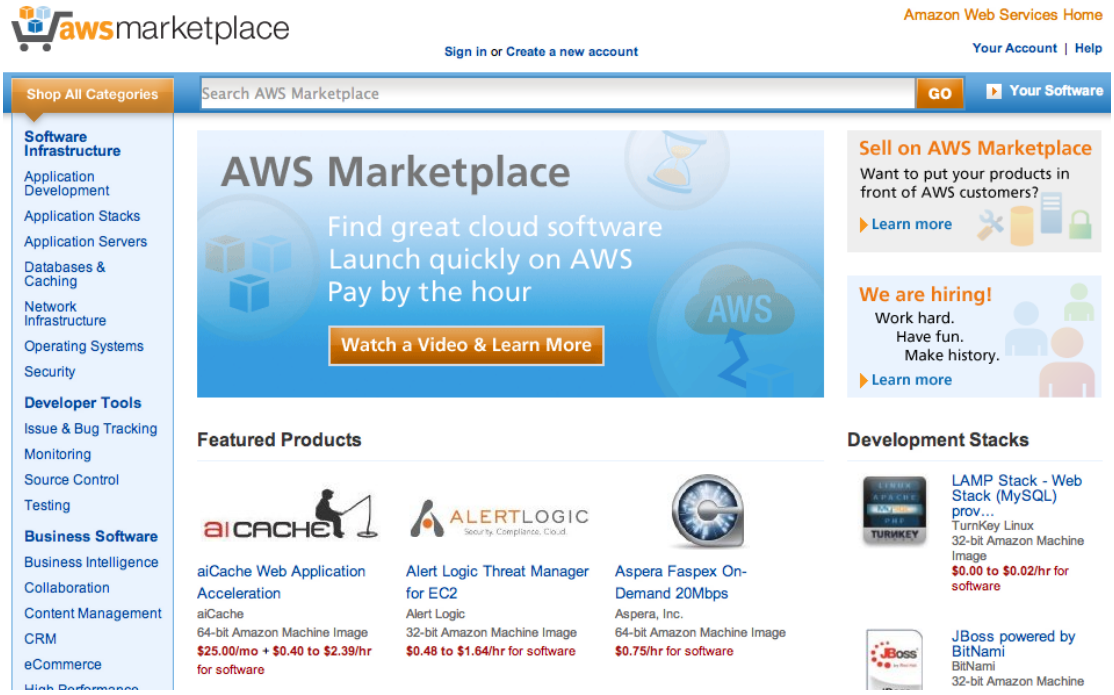
Companies who want to access Google's advanced features, like Postini email encryption (https://www.google.com/postini/encryption.html), archiving and junk email filtering need to purchase Google's services through partner resellers. These resellers are the customer's point of contact during initial migration and for any ongoing support beyond posting messages to Google's help forums.

2.1.6.2 Amazon Elastic Compute Cloud (EC2)

An additional example, from a vendor other than Google, would be Amazon Cloud services.[6]

Customers can create an EC2 account as part of signing up for Amazon web services, verifying an email address and phone number during the process. They can purchase machine instances to run on the EC2 cloud at the AWS Marketplace.[7]

[6] *https://aws.amazon.com/ec2/*
[7] https://aws.amazon.com/marketplace/



Amazon Web Services Home

Sign in or Create a new account

Your Account | Help

Shop All Categories

Search AWS Marketplace GO

Your Software

Software Infrastructure
- Application Development
- Application Stacks
- Application Servers
- Databases & Caching
- Network Infrastructure
- Operating Systems
- Security

Developer Tools
- Issue & Bug Tracking
- Monitoring
- Source Control
- Testing

Business Software
- Business Intelligence
- Collaboration
- Content Management
- CRM
- eCommerce
- High Performance

AWS Marketplace

Find great cloud software
Launch quickly on AWS
Pay by the hour

Watch a Video & Learn More

Sell on AWS Marketplace

Want to put your products in front of AWS customers?

Learn more

We are hiring!

Work hard.
Have fun.
Make history.

Learn more

Featured Products

aiCache Web Application Acceleration
aiCache
64-bit Amazon Machine Image
$25.00/mo + $0.40 to $2.39/hr for software

Alert Logic Threat Manager for EC2
Alert Logic
32-bit Amazon Machine Image
$0.48 to $1.64/hr for software

Aspera Faspex On-Demand 20Mbps
Aspera, Inc.
64-bit Amazon Machine Image
$0.75/hr for software

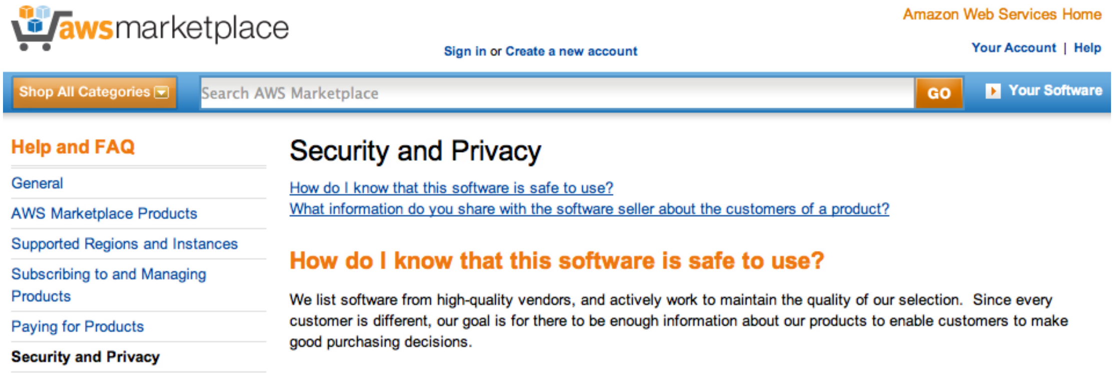
Development Stacks

LAMP Stack - Web Stack (MySQL) prov...
TurnKey Linux
32-bit Amazon Machine Image
$0.00 to $0.02/hr for software

JBoss powered by BitNami
BitNami
32-bit Amazon Machine

Figure 2: The AWS Marketplace

All machine instances are ensured for safety.



Security and Privacy

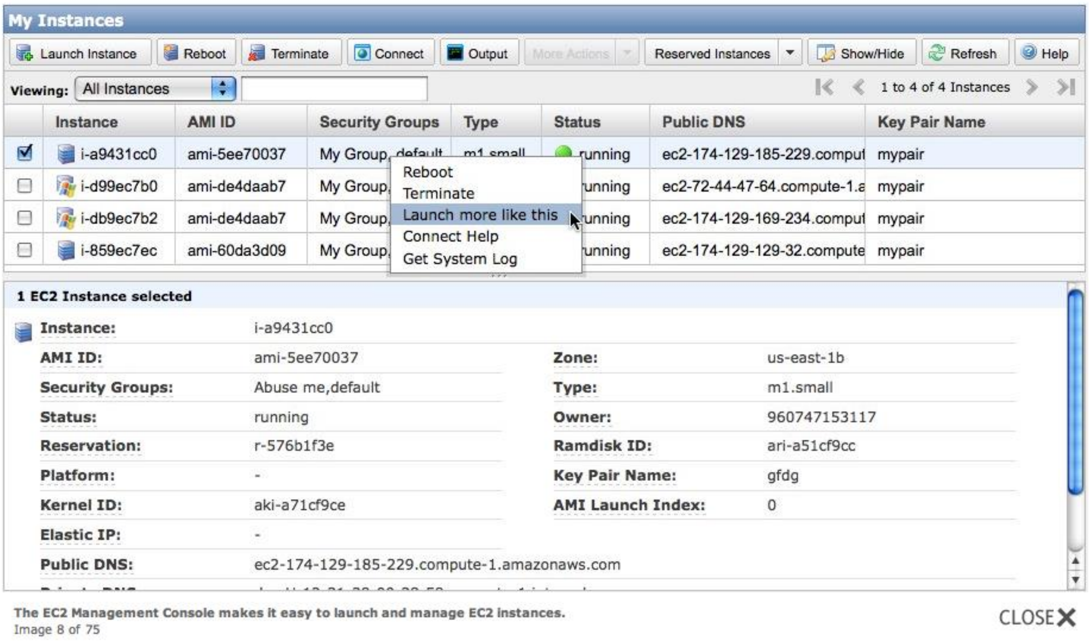
How do I know that this software is safe to use?
What information do you share with the software seller about the customers of a product?

How do I know that this software is safe to use?

We list software from high-quality vendors, and actively work to maintain the quality of our selection. Since every customer is different, our goal is for there to be enough information about our products to enable customers to make good purchasing decisions.

Figure 3: AWS Marketplace webpage about virtual machine security and privacy

Once an EC2 account has been set up, creating, starting, stopping and configuring instances is relatively easy. The account is managed through a web-based dashboard system. Users can point and click their way to a virtualised, distributed server farm.



	Instance	AMI ID	Security Groups	Type	Status	Public DNS	Key Pair Name
☑	i-a9431cc0	ami-5ee70037	My Group, default	m1.small	running	ec2-174-129-185-229.comput	mypair
□	i-d99ec7b0	ami-de4daab7	My Group,		unning	ec2-72-44-47-64.compute-1.a	mypair
□	i-db9ec7b2	ami-de4daab7	My Group,		unning	ec2-174-129-169-234.comput	mypair
□	i-859ec7ec	ami-60da3d09	My Group,		unning	ec2-174-129-129-32.compute	mypair

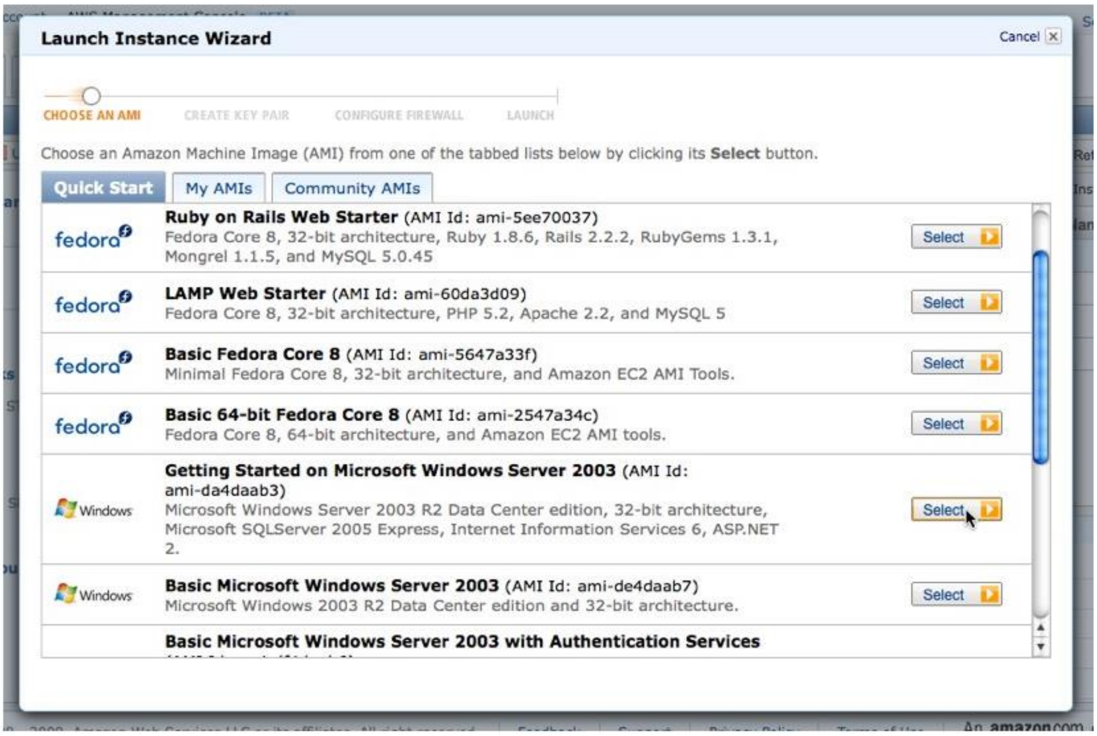
1 EC2 Instance selected

Instance:	i-a9431cc0		
AMI ID:	ami-5ee70037	Zone:	us-east-1b
Security Groups:	Abuse me,default	Type:	m1.small
Status:	running	Owner:	960747153117
Reservation:	r-576b1f3e	Ramdisk ID:	ari-a51cf9cc
Platform:	-	Key Pair Name:	gfdg
Kernel ID:	aki-a71cf9ce	AMI Launch Index:	0
Elastic IP:	-		
Public DNS:	ec2-174-129-185-229.compute-1.amazonaws.com		

The EC2 Management Console makes it easy to launch and manage EC2 instances.
Image 8 of 75

Figure 4: An example of a list of machine instances under a user's EC2 account and how they can be administered

Launching a new machine instance on the EC2 cloud is as simple as choosing an operating system and other add-ons like Ruby on Rails or Microsoft IIS from a list (Figure 5)



Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its **Select** button.

fedora **Ruby on Rails Web Starter** (AMI Id: ami-5ee70037)
Fedora Core 8, 32-bit architecture, Ruby 1.8.6, Rails 2.2.2, RubyGems 1.3.1, Mongrel 1.1.5, and MySQL 5.0.45

fedora **LAMP Web Starter** (AMI Id: ami-60da3d09)
Fedora Core 8, 32-bit architecture, PHP 5.2, Apache 2.2, and MySQL 5

fedora **Basic Fedora Core 8** (AMI Id: ami-5647a33f)
Minimal Fedora Core 8, 32-bit architecture, and Amazon EC2 AMI Tools.

fedora **Basic 64-bit Fedora Core 8** (AMI Id: ami-2547a34c)
Fedora Core 8, 64-bit architecture, and Amazon EC2 AMI tools.

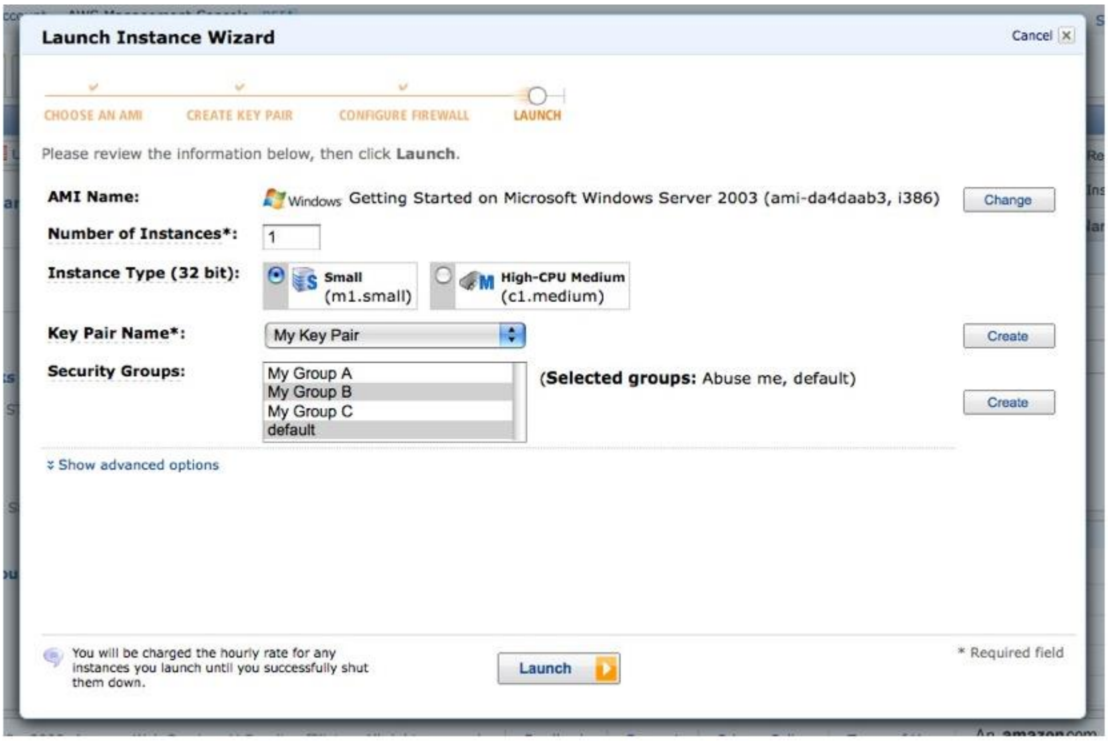
Windows **Getting Started on Microsoft Windows Server 2003** (AMI Id: ami-da4daab3)
Microsoft Windows Server 2003 R2 Data Center edition, 32-bit architecture, Microsoft SQLServer 2005 Express, Internet Information Services 6, ASP.NET 2.

Windows **Basic Microsoft Windows Server 2003** (AMI Id: ami-de4daab7)
Microsoft Windows 2003 R2 Data Center edition and 32-bit architecture.

Basic Microsoft Windows Server 2003 with Authentication Services

Figure 5: A list of available machine instances that an EC2 user could choose to launch.

After selecting a machine instance type, EC2 customers can configure that instance to be part of a security settings template, set the computational performance level and even create multiple instances from the same settings (Figure 6).



Please review the information below, then click **Launch**.

AMI Name: Windows Getting Started on Microsoft Windows Server 2003 (ami-da4daab3, i386)

Number of Instances*: 1

Instance Type (32 bit): ● Small (m1.small) ○ High-CPU Medium (c1.medium)

Key Pair Name*: My Key Pair

Security Groups: My Group A, My Group B, My Group C, default (**Selected groups:** Abuse me, default)

You will be charged the hourly rate for any instances you launch until you successfully shut them down.

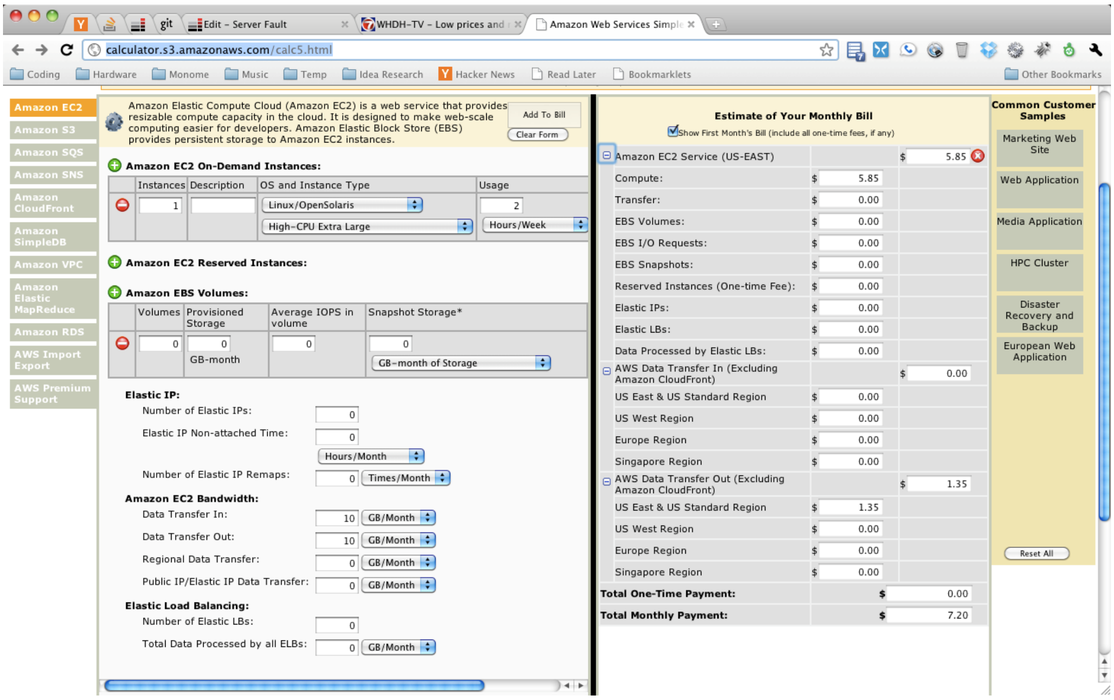
* Required field

Figure 6: The Launch Instance Wizard used when activating a machine instance on Amazon's EC2 platform.

Amazon Computing Cloud users can request additional instances at:

https://aws.amazon.com/contact-us/ec2-request/

Billing for EC2, like most cloud-based services, is based on how much processing resources, storage, and network bandwidth is used:



Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers. Amazon Elastic Block Store (EBS) provides persistent storage to Amazon EC2 instances.

Amazon EC2 On-Demand Instances:

Instances	Description	OS and Instance Type	Usage
1		Linux/OpenSolaris High-CPU Extra Large	2 Hours/Week

Amazon EC2 Reserved Instances:

Amazon EBS Volumes:

Volumes	Provisioned Storage	Average IOPS in volume	Snapshot Storage*
0	0 GB-month	0	0 GB-month of Storage

Elastic IP:

Number of Elastic IPs:	0	
Elastic IP Non-attached Time:	0	Hours/Month
Number of Elastic IP Remaps:	0	Times/Month

Amazon EC2 Bandwidth:

Data Transfer In:	10	GB/Month
Data Transfer Out:	10	GB/Month
Regional Data Transfer:	0	GB/Month
Public IP/Elastic IP Data Transfer:	0	GB/Month

Elastic Load Balancing:

Number of Elastic LBs:	0	
Total Data Processed by all ELBs:	0	GB/Month

Estimate of Your Monthly Bill

☑ Show First Month's Bill (include all one-time fees, if any)

Amazon EC2 Service (US-EAST)		$ 5.85
Compute:	$ 5.85	
Transfer:	$ 0.00	
EBS Volumes:	$ 0.00	
EBS I/O Requests:	$ 0.00	
EBS Snapshots:	$ 0.00	
Reserved Instances (One-time Fee):	$ 0.00	
Elastic IPs:	$ 0.00	
Elastic LBs:	$ 0.00	
Data Processed by Elastic LBs:	$ 0.00	
AWS Data Transfer In (Excluding Amazon CloudFront)		$ 0.00
US East & US Standard Region	$ 0.00	
US West Region	$ 0.00	
Europe Region	$ 0.00	
Singapore Region	$ 0.00	
AWS Data Transfer Out (Excluding Amazon CloudFront)		$ 1.35
US East & US Standard Region	$ 1.35	
US West Region	$ 0.00	
Europe Region	$ 0.00	
Singapore Region	$ 0.00	
Total One-Time Payment:		**$** 0.00
Total Monthly Payment:		**$** 7.20

Figure 7: A sample billing page for EC2 services, broken down by bandwidth, number of instances, data processed and other measures.

2.1.6.3 Google Compute Engine

The trainer will show the following web page on an overhead screen as an example of how someone could create and configure an instance on the Google Compute Engine: https://developers.google.com/compute/docs/hello_world. This page has instructions on how to create and configure a virtual firewall and webserver on Google's Cloud.

As a sample of how Google approaches pricing for its cloud computing engine, display this webpage: https://developers.google.com/compute/docs/pricing.

For those who might be interested in signing up for an account to get a sense of how the process works, they can visit https://developers.google.com/compute/docs/signup (the platform is an invitation-only preview as of August 2012).

3 EXERCISE COURSE

The course of this exercise is as follows. All discussions should be moderated by the trainer.

3.1 Introduction to the exercise

- Knowing the source of virtual instances running in cloud platforms and monitoring their behaviour can make the difference between safe computing and a malware-infested server leaking confidential information.

- Cloud platforms may offer in some circumstances security vulnerabilities and limitations but also enable ways to quickly respond to compromised systems.
- This exercise explores feasible scenarios, yet is still a constructed exercise. For more information, look at the *Top Threats to Cloud Computing* by the Cloud Security Alliance,[8] or the *Insider Threat Blog* of CERT/CC on the topic of cloud computing.[9]

3.2 Keys to the exercise

3.2.1 TASK 1: EXPLOITS AGAINST A CLOUD INFRASTRUCTURE

3.2.1.1 Exercise Configuration

- Trainees should work in groups of between five and six (a sixth person can act as an observer/note taker if needed to even out group sizes). Encourage the groups to include trainees from different organisations, countries and job roles to avoid one set of views or ideas dominating the group.
- Ask the trainees to select among themselves who will represent the roles and perspectives of the following people:
  - Amazon ECC technical support;
  - Northwinds IT technician;
  - AcmeCorp IT technician;
  - Estonian cloud provider support;
  - CERT representative.
- Read the incident scenario out loud to the class, and then direct the trainee groups to develop the various concepts and solutions in the 'Points of discussion' section (17.2.3.1)
- Locate the groups in break-out areas if available or at least ensure that they are sufficiently separated so their discussions don't interfere with each other.
- The trainer, assisted by a co-trainer, should visit each group in turn. Briefly answer questions from the groups if needed, allowing the trainees themselves to expound upon different possibilities and perspectives.
- The groups have four items to discuss and each item could take 10–15 minutes. The prevention section could take 20–25 minutes. Trainers may need to nudge the groups forward if they take too much time on some items. If some groups move through the items quickly, the trainers can entertain some discussion with the group, ask additional questions or make suggestions.
- Somewhere between 50–60 minutes into the discussion, lead the groups into the developing scenario events in section 17.2.3.2. This does not have to happen at the same time for each group; in fact, this won't be possible, as each group will have its own dynamic. This 'out-of-sync' approach continues until the group discussion in section 17.2.3.3 at the end of this scenario.

[8] https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[9] http://www.cert.org/blogs/insider_threat/2012/09/insider_threats_related_to_cloud_computing--installment_7_seven_proposed_directions_for_research_and.html

- Ask the trainees taking notes or another group member to present what their group has discussed before the break, preceding section 17.2.3.3.

A note about group size: groups of two are too small to have various perspectives presented in group discussion. Groups of five may lead some people to be silent while two or three trainees do all the talking. Encourage groups to be sure to review each discussion topic from the perspective of each role listed.

3.2.2 Scenario

An IT technician at Northwinds Incorporated unwittingly chooses malware-infected virtual machine instances on Amazon's Elastic Compute Cloud when he needed to create a web server for a new SQL database application. There were many options in the AWS Marketplace but a few on offer were free and from companies the technician thought were legitimate.

Unfortunately, the machine instances he chose evaded Amazon's anti-malware scanning and, in fact, were designed to intercept database and web server account credentials and relay them (and the full control over those virtual servers) to another party.[10]

When the virtual machines run, Northwinds client data is siphoned off to cloud-based storage elsewhere on Amazon's S3 platform under the control of a malicious technician who works for a competitor company, AcmeCorp. This technician registered the account using a pseudonym and it is unclear whether he is working on his own or on behalf of AcmeCorp.

Account credentials for internal databases and cloud-based email configuration are also captured.

3.1.1.1 Points of discussion

In their groups, trainees will discuss the following stages of response to the above scenario:

- Detect issue: How can we trace data leaks, unauthorized access, or other malicious activities on cloud platforms?

Just as with software from any commercial vendor or open source, cloud computing customers need to perform due diligence in evaluating the legitimacy of the source of virtual machine instances or images. There are reports of malware on Amazon's cloud: http://econsultancy.com/us/blog/8247-is-amazon-s-cloud-a-dangerous-jungle

In some cases, building their own images to run on cloud platforms or using those made from known, trusted sources may be the most secure options for cloud customers. The offline trust relationships provided by CERT communities may be useful in this.

Detecting data leaks in a cloud environment can be as simple as creating a new virtual tool—a virtualised packet sniffer. This is an example of using cloud resources to enable fast, flexible responses to attacks.

- Report issue: Who is responsible for notifying whom about the situation and how?

As listed in the ENISA ProCure Secure document on page 44 and 45, cloud customers need to monitor appropriate logs to see if any virtual server activity is unexpected. Some cloud vendors will also perform such monitoring and alert customers of a problem. In any case, Cloud computing customers need

[10] Please note that even the strongest, most sophisticated passwords would be compromised in this scenario. A virtual server could detect, perhaps by serripicious keystroke logging or packet capture programs concealed on the virtual machine, and pass along any and all usernames and passwords to the attackers.

multiple ways of contacting their vendor's security teams, not only via email, in case email systems are unavailable. CERTs can coordinate between multiple vendors and across national borders.

- Correct issue: How can we trace the path of traffic when the virtual infrastructure and software involved can spin up and disappear? Couldn't an attacker compromise a company's own cloud accounts, using it to attack yet another organisation, hiding their true identity?

See the suggested responses in the detection section above for other means to detect and correct (likely by shutting down the leaking or compromised virtual instances)

- Prevent issue in future.
  - Can expandable, dynamic cloud resources be used to combat the risks of easily created and deleted malicious virtual machines?
  - *Virtual instances of a packet sniffer and automated log collecting and parsing utilities are two examples of using cloud resources to track and alert when any anomalous activity occurs on a cloud account.*
  - How can companies obtain known-safe images of virtual machines?
  - *The convenience of creating new instances on a cloud platform means the cloud customers often do not install or configure the virtual machine images they use for their work. While cloud vendors like Amazon state that virtual machine instances are safe, numerous cases of disguised malware finding its way into curated app stores mean that we cannot be completely sure these premade instances are safe. Cloud providers and customers can also add integrity checks to VM images such as checksums and digital signatures to ensure only clean, original VM images are distributed and used.*
  - Since cloud computing uses shared resources, how does increasing usage of the cloud model affect vulnerability for non-targeted cloud customers?
  - *Using cloud resources to launch DDoS attacks mean attackers won't need to invest anything in obtaining, configuring, or running hundreds of physical servers or writing and distributing malware.*
  - *DDoS attacks against a virtual server throw so much traffic against that one server that all the other virtual servers running on the same physical host could run more slowly or go down.*
  - *The ENISA ProCure Secure document on page 42 details issues about shared cloud databases, storage, virtual network infrastructure like switches and firewalls, and hypervisor vulnerabilities. For example, when memory and storage is reapportioned, is old data securely deleted? Could a new cloud customer still access deleted data from the shared memory or storage space from a previous customer?*
  - *If a hypervisor is compromised, then all instances running on that host are also at risk.*
  - *Some mitigations are possible by opting for more separated services. Separate database instances for each customer are more secure than one database for all with customers getting access to their own records by security settings, which could be compromised by an attack like SQL Injection. In many cases, though, customers must rely on cloud providers' best practices.*
  - *As shown by the Amazon EC2 outage in April and August 2012, which took down websites for Foursquare, Quora and Reddit, cloud customers need to be sure to configure their accounts for the level of fault tolerance they can accept. This includes running instances on more than one 'availability zone' for essential services.*[11]

[11] http://money.cnn.com/2011/04/21/technology/amazon_server_outage/index.htm

3.1.1.2 Developing events for scenario

After small group discussion has progressed for 60 minutes, announce:

With Northwinds' cloud email configuration credentials also intercepted, all of Northwinds's email has suddenly been redirected to a virtualised email server that Northwinds can't access. Northwinds can't communicate via email under its own name or receive incoming emails.

The book *Hacking Exposed 7* details the 2011 attack by the group Anonymous against HBGary, a computer forensics company. 'But the *coupe de grace* was using the CEO's password to gain administrator-level privilege into HBGary's e-mail system (Google Apps), which allowed for IMAP downloading of employee inboxes. And the rest is security history—Anonymous published gigabytes' worth of e-mails from many of HBGary's employees' (p. 528). This attack began with a SQL injection against the company's web content management system.

In addition, the usefulness of cloud-based systems can have limits and issues due to security vulnerabilities. Many ISPs block SMTP traffic coming from EC2 IP addresses due to junk email activities that are not allowed by Amazon's Terms of Service but have happened anyway.[12] Google Apps for Business with Postini are sometimes mismarked as junk email by other email vendors like Yahoo.

Ask the groups to discuss the scenario developments with the focus on the following phases.

- Detect

One way that administrators could detect if cloud-based email settings are changed would be to hold regular, automated tests, sending and receiving Google Apps-based email (Gmail) to non-Google accounts. This way, if a scheduled outgoing email doesn't arrive at an external mailbox or if a scheduled incoming email to a Gmail account doesn't arrive, administrators could immediately attempt to access and to verify domain email settings.

- Report

Northwinds needs to have multiple contact methods for its Google Apps reseller (not only email) since Google does not provide direct support. Northwinds should configure email contacts for its Google Apps domain on another, non-Gmail system to facilitate regaining access.

Reaching out to the appropriate CERT team to help coordinate between the company, its service providers, and law enforcement needs to be part of Northwinds' response.

- Prevent

Using virtual images that you create yourself or that are from known, trusted sources can protect cloud infrastructure. Cloud providers and customers can also add integrity checks to VM images such as checksums and digital signatures to ensure only clean, original VM images are distributed and used.

Always having alternate email contacts on independent systems.

Lock domain transfers to limit an attacker's options to redirect traffic.

Use two-factor authentication so that compromised passwords do not compromise a critical account that could change domain settings.

Avoid using the same accounts or passwords for all of an organisation's cloud computing accounts, domain registration accounts and other critical services.

Evaluate the risks and rewards of using a cloud-based system. A company with its own, physical servers for email and DNS has direct control over these services in a crisis (but also face other vulnerabilities

[12] http://news.ycombinator.com/item?id=883622

with a lack of fault tolerance and exposure to local disasters and outages). With the Google Apps system, the company is at the mercy of Google and domain registrars for email traffic to route correctly.

When small group discussions appear to have mostly concluded, ask the trainees who took notes in the small groups (or another representative from the group) to share the groups' discussions with the whole class. If any of the sample responses above aren't covered, be sure to mention them to the class.

When all groups have shared the contents of their discussions, announce a 15-minute break. When returning from break, have the trainees come back together in one group.

3.1.1.3 Plenary discussion (20 minutes)

On page 54 of the ENISA November 2009 report Cloud Computing Risk Assessment, the 'Cloudburst' exploit against VMware and jumping access from one virtual machine to another ('VM hopping') were offered as examples of special vulnerabilities of cloud computing environments. In September 2012, Rafal Wojtczuk and Jan Beulich discovered another exploit that allows arbitrary code to run, jumping outside of the boundaries of a virtual machine, and attacks the Xen hypervisor using a particular memory corruption issue.[13]

Solicit comments from all trainees.

- What special security issues arise in a cloud environment based on your group discussions? Are there any we haven't thought of?
- What about the layers of technology that enable cloud computing? How do they interact to improve or reduce reliability?

The cloud is based on virtualisation and virtual machines and shared data stores that are easy-to-replicate and migrate to multiple datacentres. All the vulnerabilities of these foundation technologies are part of the cloud's weaknesses. Any exploit against virtualization techniques, like a hypervisor attack, are part of cloud vulnerability. Any lack of redundancy in infrastructure like both of datacentre's Internet links going through the same underground trunk line will affect cloud fault tolerance.

3.1.2 TASK 2: Cloud data flexibility and control (30 min)

> *A pharmaceutical company contracts with a hosted database provider to maintain and back up its drug trial patient records. Unbeknownst to the company, the database provider uses Google Cloud Storage to maintain fault tolerant access for the provider's database platform. The Cloud Storage is configured to automatically move among Google's datacentres to minimise latency when the database is accessed by end users.*
>
> *The company's IT department has not restricted add-on apps can run for their employees, as well as how the hosted database is accessed by these apps. A salesperson of the pharmaceutical company uses Google web apps to funnel data from the company's hosted database into a live dashboard to show potential European government clients.*

3.4.4.1 Small group discussion

Break the class into groups of five trainees each. (These can be the same groups as in 1.2.1 or new groupings.) As before, the trainer(s) should circulate among the small groups to provide brief answers to questions and guide discussion along the lines of the topics to follow.

[13] http://www.vupen.com/blog/20120904.Advanced_Exploitation_of_Xen_Sysret_VM_Escape_CVE-2012-0217.php

Ask the trainees to select among themselves who will represent the role and perspective of the following people:

- the pharmaceutical company representative, trying to demonstrate the capabilities of his company's system to European health ministry officials;
- the IT support technician of the pharmaceutical company, well-versed in the health care data privacy laws in the United States and relatively new to using a cloud-distributed database;
- a vendor of distributed database who uses Google-based storage, something the pharmaceutical company doesn't know, and is a Google reseller;
- a patient data privacy advocate;
- a CERT representative.

Ask the groups to discuss the following questions and issues:

- Detect issue: What determines which country's data privacy and security laws apply – Where the data is stored? Where it is accessed? Where data is processed?

Typically, where data is stored, where it is accessed, and where it is processed determine which country's laws apply. However, with the distributed nature of cloud computing, data storage, access, and processing could happen in multiple jurisdictions.

Also note that the base of a cloud provider's business may determine what actions that company takes. Microsoft, for example, in 2011 said it would comply with US Government requests for data even if the information belonged to an EU citizen and it was stored on a non-US-based server.

Again, regular log monitoring may assist in knowing where cloud-based data is. Cloud account dashboards may also give this information. IT technicians may need to use IP address blocking to restrict from where data can be accessed.

- Report issue: Who needs to respond to cloud-based security breaches? The cloud provider or its clients? What if clients can't tell when vendors use cloud computing or storage for backend services? What about those patients whose information may have been accessed?

With so many variables about where cloud-based data may be stored and used, coordinating responses during an incident is especially tricky. Reaching out to the relevant CERTs will help bring together vendors, customers, and other entities.

It is quite possible, especially with SaaS web applications like Gmail or the web-based database in this scenario, that customers would not know that underlying storage has been farmed out to a cloud storage vendor. Performing proper due diligence, reviewing audits and logging are all critical in monitoring the activities of a cloud service provider as detailed in the ENISA ProCure Secure document referenced earlier.

- Prevent issue in future: What are ways to mitigate security risks when sensitive or legally protected data is stored and accessed from the cloud?

Some providers like VPS.net allow their customers to choose which datacentres are used to store their data and processing among several countries.

In some cases, even though cloud systems offer flexible access and better fault tolerance, some data may just be better protected on physical hardware under the direct control of an organisation's IT department.

Administrators can restrict access to portions of the cloud systems, such as allowing Gmail but disabling Google Sites, Docs, and the App Marketplace for end users.

4 EVALUATION METRICS

Evaluating the results of this exercise, the trainer should take into consideration the class's understanding of these key concepts.

- Define Cloud computing: distributed, virtualised or the US NIST's criteria of on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.
- Define Cloud computing service models SaaS, PaaS, and IaaS
- Note the importance of knowing whom to contact given the type of cloud service provided. As an example, a Google Apps for business customer needs to work through the Google reseller company for support beyond posts in a help forum. A web application front end could be using another company's cloud storage or computing options for back end services. Outages and vulnerabilities in those back end services can affect cloud customers.
- Due diligence and audit may be the only ways to know where data is stored and used or to know if a breach has occurred. Regular monitoring and testing can aid in detection of an incident.
- Having non-cloud based backup systems, as simple as an email account through another provider, will allow for easier communications if cloud systems are compromised.
- As in all of IT, we must balance the risk and rewards of cloud computing on top of the edges of legal requirements and budgetary realities to find the best course for our organisation's work.

5 REFERENCES

1. Pepitone, Jennifer, *Amazon EC2 outage downs Reddit, Quora*, CNN Money, 22 April 2011. (http://money.cnn.com/2011/04/21/technology/amazon_server_outage/index.htm)
2. Savitz, Eric, '*Can European Firms Legally Use U.S. Clouds To Store Data?*', Forbes, 2 January 2012 (http://www.forbes.com/sites/ciocentral/2012/01/02/can-european-firms-legally-use-u-s-clouds-to-store-data/) [Concise analysis of impact of US laws that require US companies to comply with US government data requests regardless of where the data is located and not to disclose those requests in some cases, conflicting with EU disclosure requirements.]
3. Cloudburst demonstration, Kortchinsky, Kostya (http://www.immunityinc.com/documentation/cloudburst-vista.html)
4. Cloud Computing ENISA web portal: (http://www.enisa.europa.eu/activities/application-security/cloud-computing/introduction-to-cloud-computing)
5. *Cloud Computing Risk Assessment*, ENISA, 20 Nov 2009 (http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment)
6. Cloud Computing video, ENISA (http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing)
7. Gill, Kulvinder, *Data Jurisdiction in the Cloud: The Patriot Act Fear Factor*, EzeCastle Integration Hedge IT Blog, 26 June 2012. (http://www.eci.com/blog/310-data-jurisdiction-in-the-cloud-the-patriot-act-fear-factor.html)

8. Ormandy, Tavis, *An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments* (http://taviso.decsystem.org/virtsec.pdf)
9. Hardenburgh, Ian, *Getting started with the Google App Engine*, TechRepublic, 9 August 2012 (http://www.techrepublic.com/blog/datacenter/getting-started-with-the-google-app-engine/5724)
10. Rodrigues, Thoran, *Hardening the cloud: New security tools help to seal the gaps*, Tech Republic, 1 August 2012. (http://www.techrepublic.com/blog/datacenter/hardening-the-cloud-new-security-tools-help-to-seal-the-gaps/5703)
11. Clark, Jack, *How Google Compute Engine hopes to sidestep AWS failures*, ZDNet, 23 July 2012 (http://www.zdnet.com/google-compute-engine-hopes-to-sidestep-aws-failures-7000001379/)
12. Caruso, Jeff, *IaaS vs. PaaS vs. SaaS*, *Network World*, 2 November 2011. (http://www.networkworld.com/news/2011/102511-tech-argument-iaas-paas-saas-252357.html)
13. Software Engineering Institute at Carnegie Mellon University, *Insider Threats Related to Cloud Computing--Installment 5: Securing Against Cloud-Related Insiders*, Insider Threat Blog, 27 August 2012 (http://www.cert.org/blogs/insider_threat/2012/08/insider_threats_related_to_cloud_computing--installment_5_securing_against_cloud-related_insiders.html) [Note: the other four instalments in this blog series also address important cloud computing security issues like using the cloud to conduct malicious activity in Instalment 4 and exploiting cloud weaknesses in Instalment 3.]
14. ENISA *Online as soon as it Happens*, 8 February 2010 (https://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/onlineasithappens/at_download/fullReport)
15. Cheah, Gigi; Tan, Jeremy; and Rose, Norton, *Potential data jurisdiction problems for cloud service users,* Asia Cloud Forum, 6 June 2012. (http://www.asiacloudforum.com/content/potential-data-jurisdiction-problems-cloud-service-users)
16. ENISA*, Procure Secure: A guide to monitoring of security service levels in cloud contracts*, 2 April 2012. (http://www.enisa.europa.eu/activities/application-security/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts)
17. Rodrigues, Thoran, *Side-by-side comparisons of IaaS service providers*, TechRepublic, 7 August 2012 (http://www.techrepublic.com/blog/datacenter/side-by-side-comparisons-of-iaas-service-providers/5717) [This article includes links to major providers as well as points of comparison among them.]
18. ENISA, *Survey and analysis of security parameters in cloud SLAs across the European public sector*, 21 December 2011. (http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector)
19. Binning, David, *Top five cloud computing security issues*, Computerweekly.com, 24 April 2009 (http://www.computerweekly.com/news/2240089111/Top-five-cloud-computing-security-issues)
20. Ranger, Steve, *US, UK dominate world's SaaS spending*, ZDNet, 8 August 2012. (http://www.zdnet.com/us-uk-dominate-worlds-saas-spending-7000002332/)

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu