Incident handling in the cloud

Toolset, Document for students

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

Copyright Notice

Table of Contents

1 What Will You Learn

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 even to any one set datacentre—a normal situation that occurs in cloud computing solutions.

The growing prominence of cloud computing presents some new security challenges, some that are "back to the future" and some that are common to any computing environment. But what is this "cloud" thing anyway and why does it seem to dominate IT journalism and seem to be applied to every project plan during the last few years?

2 Exercise Task

2.1 Task 1 Exploits against a Cloud Infrastructure

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 offers 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 intercept database and web server account credentials and relay them (and the full control over those virtual servers) to another party.

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.

Roles in the scenario:

- Amazon ECC technical support
- Northwinds IT technician
- AcmeCorp IT technician
- Estonian cloud provider customer support
- CERT representative

Points of discussion:

- Detect issue: How can we trace data leaks, unauthorized access, or other malicious activities on cloud platforms?
- Report issue: Who is responsible for notifying whom about the situation and how?

- 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 his true identity?
- Prevent issue in future:
  - Can expandable, dynamic cloud resources be used to combat the risks of easily created and deleted malicious virtual machines?
  - How can companies obtain known-safe images of virtual machines?
  - Since cloud computing uses shared resources, how does increasing usage of the cloud model affect vulnerability for non-targeted cloud customers?

2.2 Task 2: Cloud data Flexibility and control

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 minimize 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.

Roles in the scenario:

- 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.
- Vendor of distributed database who uses Google-based storage, something the pharmaceutical company doesn't know, and is a Google reseller
- Patient data privacy advocate
- CERT representative

Discussion Questions

- 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?

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

3 Conclusion

Cloud computing offers revolutionary flexibility in creating a distributing architecture for software, processing and storage, as well as network infrastructure. But with this flexibility, system administrators must also be aware of the dangers when running virtual machine instances whose origins might be unknown or their behaviour untested. Lacking direct, physical access to data or to the machines processing it in the cloud, also means that having good contact information in case of emergency, proper vetting of vendors, ongoing monitoring and testing and pre-staging non-cloud backup systems are all vital considerations before migrating to cloud platforms.

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