Stay in control!

How Moving to the Cloud Really Changes Your Security Requirements
Jeroen Vandeleur

- Focus on security architecture and infrastructure
- Continuous security monitoring
- Incident manager @ NVISO CSIRT
- Internal IT Manager

+32 (0) 492 94 56 91
jvandeleur@nviso.be
www.linkedin.com/in/vandeleurjeroen
How it all started
How it all starts
Roadmap meeting with the CEO

We need to go to the next level!
We need to reduce costs and achieve business agility.

You can do this!
How it all starts
Our key priorities

Business priorities

- Reduce Total Cost (TCO)
- Increase User Experience
- Increase Revenue
- Achieve business agility
- “Remain in control”

And as a security company we have a 5th driver
But ... Is it secure?
Cloud service providers follow a shared responsibility model where the CSP is responsible for the “security of the cloud” while the cloud consumer is responsible for the “security in the cloud”.

<table>
<thead>
<tr>
<th>Component</th>
<th>On - Prem</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Data</td>
<td></td>
<td>MS</td>
<td>MS</td>
<td>MS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AWS</td>
<td>AWS</td>
<td>AWS</td>
</tr>
<tr>
<td>Client &amp; end-point protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity &amp; access management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Shared responsibility model
Microsoft

PDF with 10 pages of detailed information
Shared responsibility model
Amazon

Want More Information About The Shared Responsibility Model?

Contact Us

If you would like access to AWS compliance reports, please use AWS Artifact Artifact homepage. If you have questions, please complete the form below a
An asterisk (*) indicates required information.

* First Name:

* Last Name:

* Business Email Address:

* Job Role:
  Select...

* Phone Number:
  (000) 000-0000

* Company Name:

Company Size:
  Select...

* Industry:
  Select...
Security breaches in the cloud

What can go wrong?

Dropbox hack leads to leaking of 68m user passwords on the in

Data stolen in 2012 breach, containing encrypted around two-thirds of cloud firm’s customers, has

Dow Jones data leak: Over 2 million customers' personal details exposed in cloud storage error

The cloud leak comes a week after a third-party vendor exposed millions of Verizon subscribers' records.

By Hyacinth Mascarenhas
July 18, 2017 07:14 BST

A CIO’s worst nightmare: When your cloud provider goes bankrupt

By Derek du Preez January 6, 2015

SUMMARY: Paul Golland, CIO of the north-east London borough of Waltham Forest, in early 2013 faced a crisis that I’m sure all CIOs would never wish to go through – being told that your sole cloud provider is going into administration and that you have 24 to 48 hours to get your business’ data and systems [...]

A CIO’s worst nightmare: When your cloud provider goes bankrupt

By Derek du Preez January 6, 2015

SUMMARY: Paul Golland, CIO of the north-east London borough of Waltham Forest, in early 2013 faced a crisis that I’m sure all CIOs would never wish to go through – being told that your sole cloud provider is going into administration and that you have 24 to 48 hours to get your business’ data and systems [...]
YOU NEED TO DO BETTER!

YOU ARE HERE FOR THE MANUAL
This guide consists of 4 main chapters!

Chapter 1: Prepare for the cloud
Chapter 2: Cloud Features & POCs
Chapter 3: Migration to the Cloud
Chapter 4: Cloud Operational Model
CHAPTER 1 – Prepare for the cloud
Approaching the big move

1.1 Use a data-centric approach in stead of the traditional perimeter approach

1.2 Identify functional and non-functional requirements

1.3 Know your environment! (Data & asset classification)
# What do you need to know

Approaching the big move

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.4</strong></td>
<td>Define your trust model</td>
<td></td>
</tr>
<tr>
<td><strong>1.5</strong></td>
<td>Identify the main threats to your environment</td>
<td></td>
</tr>
<tr>
<td><strong>1.6</strong></td>
<td>Define your list of security controls</td>
<td></td>
</tr>
</tbody>
</table>
Build trust models

Based on your identification you can build trust models

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>1.2</td>
<td>1.3</td>
<td>1.4</td>
<td>1.5</td>
</tr>
</tbody>
</table>

**Trust Models**

<table>
<thead>
<tr>
<th>User Type</th>
<th>Employees / partners / clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust level</td>
<td>Not trusted / semi trusted / trusted</td>
</tr>
<tr>
<td>Allowed access</td>
<td>Public, internal, secret &amp; confidential data</td>
</tr>
<tr>
<td>Req Sec Controls</td>
<td>Your list of security controls</td>
</tr>
</tbody>
</table>
PHASE 2 – Cloud features & POCs

Project phases

CHAPTER 2 – Cloud features & POCs

Chapter 1
Prepare for the cloud

Chapter 2
Cloud Features & POCs

Chapter 3
Migration to the Cloud

Chapter 4
Cloud Operational Model
Challenge 1 - Picking the cloud model that’s right for us

Cloud service model

2.1

Select your cloud service model and deployment

IaaS in private deployment?

Test Cases: 11% *

Management: ↓

Security: ↑

Service Cost: ↑

* Minimal configuration
Challenge 1 - Picking the cloud model that’s right for us

2.1 Select your cloud service model and deployment

SaaS in public deployment?

Test Cases

- 29% *

Management

Security

Service Cost

* Minimal configuration
Challenge 1 - Picking the cloud model that’s right for us

Cloud service model

2.1 Select your cloud service model and deployment

Combination between IaaS & SaaS in hybrid deployment?

Test Cases
- 55% *

Management

Security

Service Cost

* Minimal configuration
Challenge 2- Cloud access controls

Access controls

2.2 Review your authentication model

Multiple solutions are available and integrated in your cloud environment but manual configuration is needed

- Multi-factor authentication
- Conditional access
- Certificate based authentication

SaaS Solution

IaaS Solution
Challenge 3 – Data classification policy

Data classification toolset

2.3

Enable data protection controls based on the classification

Data protection is integrated in our cloud solution, certificate management is done by the cloud provider.

Workstation application and plugin

Central configuration and enforcement
Challenge 3 – Device Management

Trust vs non-trusted

2.4

Configure Mobile Device Management and enforce policies

Mobile device management is out of the box and is easier to manage trust relationships to all your services.

Mobile Device Management
Mail on BYOD
Compliancy checks
Challenge 4 - Data leakage

2.5 Enable and configure data loss prevention rules

No need for dedicated solution because data loss prevention can be configured via the information protection policy

Labelling
File encryption based on user access
Exchange transaction rules
Challenge 5 - Continuous security monitoring
Centralized logs

2.6 Configure cloud logging and auditing

So many dashboards, so little time ....
Multiple dashboards in different views and it becomes difficult to manage.
Penetration testing in the cloud means a different approach! You need to involve your cloud provider and create a test approach for your environment.

Providers’ approval (Rules of engagement)
Increase of your Cloud invoice
Carefully select Your assets
Validate your dashboards and logs
Chapter 3: Migration to the Cloud

Project phases

Chapter 3: Migration to the cloud

Chapter 1
Prepare for the cloud

Chapter 2
Cloud Features & POCs

Chapter 3
Migration to the Cloud

Chapter 4
Cloud Operational Model
Moving towards the cloud
A man with a plan!

3.1 Define Migration plan

**Week 1**
- POC settings to PRD

**Week 2**
- List users
- Locate assets
- Transfer data owner

**Week 3**
- Data validation
- Mail validation
- Workstation Mig.

**Week 4**
- Support & operations
- List issues

Partial test
Full test-run
Full Migration
Moving towards the cloud
A man with a plan!

3.2 Migration process

- POC settings to PRD
- List users
  - Locate assets
  - Transfer data owner
- Data validation
  - Mail validation
  - Workstation Mig.
- Support & operations
  - List issues

- Data ownership changed
- Mail & data throttling
- Migration time for data transfer
- Folder path < 255 characters
- Conditional access issues
- MS teams (roll-back)
CHAPTER 4 – Cloud Operational Model
## Cloud Operational model

### Support and management

<table>
<thead>
<tr>
<th>4.1</th>
<th>Maintenance and management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Increase in functionality = increase in day to day management</td>
</tr>
<tr>
<td></td>
<td>Define update and patch management (IAAS)</td>
</tr>
<tr>
<td></td>
<td>Cost management (based on usage metrics)</td>
</tr>
<tr>
<td></td>
<td>Structured approach towards service onboarding &amp; increase our security posture</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Service Design</th>
<th>Service Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGMT Meeting</td>
<td>Security Architecture Board</td>
<td>Service Improvement meeting</td>
</tr>
<tr>
<td></td>
<td>Service line Board</td>
<td>Weekly status Calls</td>
</tr>
</tbody>
</table>
Risk and security monitoring
Detect vulnerabilities and incidents

4.2

Continuous security monitoring

O365 - Risk Monitor
Take Action, Improve Your Score

TARGET SCORE
356
26 actions

BALANCED
These actions cover the basics, and include some defense in depth choices.

82
Current score

452
Max. Score

26 Actions in the queue
Your pending Secure Score is: 356

Vulnerability Management

Security Monitoring

- Eagle Eye - Menu - dashboards
- Cyber Threat Intelligence | IDS alerts | Outliers | YARA | File analysis | DNS traffic | HTTP traffic | Netflow | Windows events | Health
- WinrevFilter - EventID:0x: Descending
- WinrevFilter - Top Event ID:

31,713
Total events

- No security alerts
- No attacked resources to display
Incident response
How to do incident response in cloud environments

4.3 Prepare for incidents

- Understand your service provider
  - Shared responsibility model
- Validate acquisition procedure in your cloud model
- Create an incident response plan for cloud environments
- Validate New features
  (e.g. Azure Security Center investigate incidents in Preview)

Incident Response
Using Microsoft Defender ATP

Windows Defender Security Center | Security operations dashboard

<table>
<thead>
<tr>
<th>Active alerts</th>
<th>30 days</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Alerts" /></td>
<td><img src="image" alt="Alerts" /></td>
</tr>
<tr>
<td><strong>6</strong> New</td>
<td><img src="image" alt="Alerts" /></td>
</tr>
<tr>
<td><strong>1</strong> In progress</td>
<td><img src="image" alt="Alerts" /></td>
</tr>
<tr>
<td>01.19.2018</td>
<td>Microsoft command-line utility Regsvr32.exe launched suspicious commands.</td>
</tr>
<tr>
<td>01.19.2018</td>
<td>A process was injected with potentially malicious code</td>
</tr>
<tr>
<td>01.19.2018</td>
<td>Suspicious Powershell commandline</td>
</tr>
<tr>
<td>01.19.2018</td>
<td>Suspicious Powershell commandline</td>
</tr>
</tbody>
</table>

Machines at risk
- nviso-win10-sre
- nviso-win10-jva
- nviso-win10-msa

Users at risk
- nviso\sreynaert
- nviso\jvandeleur
- nviso\msmaris
LESSONS LEARNED
<table>
<thead>
<tr>
<th></th>
<th>Lessons learned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Talk to your industry peers</td>
</tr>
<tr>
<td>2</td>
<td>Build your cloud on trust models</td>
</tr>
<tr>
<td>3</td>
<td>Choose wisely (Service &amp; deployment models)</td>
</tr>
<tr>
<td>4</td>
<td>Do a POC with selection of users for a longer period</td>
</tr>
<tr>
<td>5</td>
<td>Multiple migration test runs</td>
</tr>
<tr>
<td>6</td>
<td>Moving to the cloud = decrease workload</td>
</tr>
<tr>
<td>7</td>
<td>READ the weekly update mail 😊</td>
</tr>
</tbody>
</table>
Thank you!

Hacked? Malware? Need urgent support?
Call us: +32 (0)2 588 43 80
Mail us: incidents@nviso.be