Shadow Cloud Discovery

ISACA Fokus Event

30. November 2015
Contents

01 Risks of Shadow Cloud Usage
02 Our Approach
03 Contact Us
Risks of Shadow Cloud Usage
Selection of most relevant risks

1. **Data security**
   - Employees share data with unauthorised third parties
   - Data loss and data misuse incidents may remain undetected

2. **Financial**
   - Penalties due to violation of contracts, laws and regulation
   - Multiple service fees and inefficiencies due to multiple contracts

3. **Governance**
   - Unknown criticality of shadow cloud for business processes
   - Insufficient monitoring, reporting and control system

4. **Compliance**
   - Non-Compliance to internal and external regulations
   - Data resides within different jurisdictions and protection levels
Our Approach
Project Structure (outline)

The estimated duration of a Shadow Cloud Discovery project is between 5 and 10 days, depending on the environment.
**Our Approach**

Topics to be covered during Initial Workshop

**Aim of the Initial Workshop**

- Define objectives and evaluation priorities
- Understand the IT landscape and IT organisation
- Clarify on known and relevant shadow cloud related risks
- Identify stakeholders
- Identify contact persons for log extraction, interviews etc.
- Understand security measures already implemented
- Analyse cloud strategy including e.g. approved cloud services
Our Approach
Log File Content required for Shadow Cloud Discovery

**Required Data**

- Source IP*
- Destination IP/Hostname
- Action (Allow/Block)
- Timestamp (Date and Time)
- Traffic (up/down)

**Optional Data**

- User Name
- Request Method (GET/POST)
- Response Code
- User Agent (Browser-Type)
- File Type (MIME/Content-Type)

**Formats**

- .csv
- Syslog
- .txt
- .xls
- .xlsx
- .pdf

* IP-Addresses and user names can be pseudonymised or anonymised by measures taken by customer or PwC; to be agreed individually prior to processing.

** These information can be processed solely by Tool 2 (see next slide).

Based on a log extract (few hundred rows), we configure the tool to match the individual structure and content of the log file.


PwC
Our Approach
Overview of the Tools used for the Log-Analysis

**Tool 1 - offline**

✓ Tool can be installed locally on physical or virtual machine provided by customer or PwC
✓ Tool operates with repository of Cloud Services including risk assessment and further details
✓ Tool provides results within a static report (pdf) incl. risk ranking, usage behaviour etc.

**Tool 2 - online**

✓ Software connector installed on PwC hardware extracts data related to shadow cloud usage
✓ Sensitive data can be removed or tokenised prior to the encrypted upload to online tool
✓ Analysis provides deep and detailed insights into usage behaviour, related risks etc.

Easy configuration leads to short ramp-up phase and quick results

Additional drill-downs allow for further in-depth analysis of cloud usage

PwC
Our Approach
The Result – Foundation for further Project Work

What a Discovery report can contain (example)

### Contents

- 01 Management Summary
- 02 Introduction and Project
- 03 Risks and Security Measures
- 04 Results and Fields of Action

### Top 10 High Risk Cloud Services Accessed

<table>
<thead>
<tr>
<th>No</th>
<th>Cloud Service Provider</th>
<th>Category</th>
<th>Service Risk Score</th>
<th>Access Attempts</th>
<th>Allowed Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Daily Motion</td>
<td>Content Sharing</td>
<td>7 (High)</td>
<td>2499</td>
<td>100%</td>
</tr>
<tr>
<td>2</td>
<td>Online Video Cutter</td>
<td>Collaboration</td>
<td>7 (High)</td>
<td>710</td>
<td>100%</td>
</tr>
<tr>
<td>3</td>
<td>Pdfzip.net</td>
<td>Collaboration</td>
<td>7 (High)</td>
<td>675</td>
<td>100%</td>
</tr>
<tr>
<td>4</td>
<td>ConvertICO</td>
<td>Collaboration</td>
<td>7 (High)</td>
<td>616</td>
<td>100%</td>
</tr>
<tr>
<td>5</td>
<td>YUDU Media</td>
<td>Media</td>
<td>7 (High)</td>
<td>335</td>
<td>100%</td>
</tr>
<tr>
<td>6</td>
<td>Source-Forge</td>
<td>Development</td>
<td>7 (High)</td>
<td>309</td>
<td>100%</td>
</tr>
<tr>
<td>7</td>
<td>PHP</td>
<td>Development</td>
<td>7 (High)</td>
<td>167</td>
<td>100%</td>
</tr>
<tr>
<td>8</td>
<td>OpenClipart</td>
<td>Collaboration</td>
<td>7 (High)</td>
<td>164</td>
<td>100%</td>
</tr>
<tr>
<td>9</td>
<td>Mega</td>
<td>Cloud Storage</td>
<td>7 (High)</td>
<td>138</td>
<td>100%</td>
</tr>
<tr>
<td>10</td>
<td>Imgflip</td>
<td>Content Sharing</td>
<td>7 (High)</td>
<td>111</td>
<td>100%</td>
</tr>
</tbody>
</table>

June 2015


PwC
Our Approach
Exemplary service modules deliverable based on Discovery

PwC Shadow Cloud Discovery Services: Discover the extent of your company’s shadow cloud usage and start governing all public cloud services in use!

- Uncover and analyse the shadow cloud services used in the company
- Analyse criticality of selected shadow cloud services for IT & business
- Examine internal control system and determine cloud coverage
- Identify compliance gaps & regulatory risks and assess potential impact
- Coach users and management to raise awareness for shadow cloud risks
- Strengthen cloud governance and enhance monitoring & reporting
Contact information

Markus Vehlow  
Partner  
Risk Assurance Solutions  
Tel. +49 160 7139416  
markus.vehlow@de.pwc.com

Aleksei Resetko  
Senior Manager  
Risk Assurance Solutions  
Tel. +49 151 14268214  
aleksei.resetko@de.pwc.com

Immo Regener  
Senior Consultant  
Risk Assurance Solutions  
Tel. +49 151 46714572  
immo.regener@de.pwc.com

Moritz Roos  
Consultant  
Risk Assurance Solutions  
Tel. +49 160 90117325  
moritz.roos@de.pwc.com