Information Security & the Cloud

Matthew A. Titcombe, CISSP
CEO & Sr. Information Security Consultant
Obligatory Overview

• A bit about me
• What is the Cloud?
• Where is the Cloud?
• What Kind of Clouds are there?
• Who is responsible for the Cloud?
• What are the risks of “going to the Cloud”?
• Should we use the Cloud?
• How can we protect ourselves?
A Bit About Me

• Started in IT back in 1990
• 1st Information Security Incident in 1999
• Network/Security Architect for Epsilon in 2001
• Air Force & DoD Enterprise & Information Security Architect
• Air Force Program Manager at SAF/CIO and Air Force Academy
• Started Peak InfoSec in 2016
What is the Cloud?

• **Cloud** computing is a general term for anything that involves *delivering hosted services* over the Internet.
  - Original “Cloud” services were Domain Name Services (e.g., [www.apple.com](http://www.apple.com) = 17.140.160.59)
  - Web-site hosting

• The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams.
# Where is the Cloud?

<table>
<thead>
<tr>
<th>Private Cloud</th>
<th>Public Cloud</th>
<th>Hybrid Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>A cloud computing model in which an enterprise uses a proprietary architecture and runs cloud servers within its own data center. Also known as “On-premise”</td>
<td>A cloud computing model that includes a mix of on-premises, private cloud and third-party public cloud services with orchestration between the two platforms.</td>
<td>A cloud computing model in which a third-party provider makes compute resources available to the general public over the internet. With public cloud, enterprises do not have to set up and maintain their own cloud servers in house.</td>
</tr>
</tbody>
</table>

**CHARACTERISTICS:**
- Single-tenant architecture
- On-premises hardware
- Direct control of underlying cloud infrastructure

**TOP VENDORS:**
HPE, VMware, Dell EMC, IBM, Red Hat, Microsoft, Open Stack

**CHARACTERISTICS:**
- Cloud bursting capabilities
- Benefits of both public and private environments

**TOP VENDORS:**
A combination of both public and private cloud providers

**CHARACTERISTICS:**
- Multi-tenant architecture
- Pay-as-you-go pricing model

**TOP VENDORS:**
AWS, Microsoft Azure, Google Cloud Platform
# What kinds of Clouds are there?

<table>
<thead>
<tr>
<th>Infrastructure-as-a-Service</th>
<th>Platform-as-a-Service</th>
<th>Software-as-a-Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>A model in which a third-party provider hosts servers, storage and other virtualized compute resources and makes them available to customers over the internet.</td>
<td>A model in which a third-party provider hosts application development platforms and tools on its own infrastructure and makes them available to customers over the internet.</td>
<td>A software distribution model in which a third-party provider hosts applications and makes them available to customers over the internet.</td>
</tr>
</tbody>
</table>

**EXAMPLES:**
- AWS, Microsoft Azure and Google Compute Engine
- AWS Elastic Beanstalk, Google App Engine and SalesForce
- Microsoft Office 365, Salesforce, NetSuite and Concur

**REAL WORLD EXAMPLE:**
- Empty Warehouse
- Warehouse with shelves, forklifts, power, etc
- Amazon storefronts
<table>
<thead>
<tr>
<th></th>
<th>On Premise</th>
<th>Infrastructure-as-a-Service</th>
<th>Platform-as-a-Service</th>
<th>Software-as-a-Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Code</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Middleware</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtualization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personnel Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Who is responsible for the Cloud? You

Cloud Service Provider
What are the risks of “going to the Cloud”? You are being targeted...

During September, one of our clients had 8,453 failed login attempts to their Office 365 accounts.
What are the risks of “going to the Cloud”? 

1. **Your Cloud Administrator leaves your system unsecured**
   - “Private AWS” instances left unsecured without username/password and open to the Internet

2. **Your information is accessible from anywhere**
   - Users (& Hackers) can download your info to their personal unsecured/compromised devices

3. **You give up your data rights**
   - Many SMB’s use Google’s GMAIL not realizing they have rights to posted content

4. **The Cloud Service Provider & your data is breached**
   - BenefitMall (akin to ADP) was breached in 2019. The breach may have included customer names, addresses, Social Security numbers, dates of birth, bank account numbers, and information on the payment of insurance premiums

5. **Can’t Access the Cloud Service Provider**
   - Your business can’t operate because employees can’t get to time-sensitive, critical data

6. **The Cloud Service Provider’s engineer sells your data**
   - AWS employee sold 100 Million accounts on the Darkweb from Capitol One plus an undisclosed information from 30+ other businesses
Should we use the Cloud?

• The Short Answer: Yes

• Long Answer:
  • ABSOLUTELY for Utility services like Office 365
    • Cloud Service Providers secure their systems better than your local IT companies ever can
  • MAYBE for niche Cloud Service providers
    • Too many cases of a small Cloud Service Provider running in Amazon, et al, and claiming all of the “Big-fishes” security credentials
  • NO for critical data that runs processes on premise
    • More common for industrial, research & development, and specialized businesses
How can we protect ourselves?

- Use Multi-Factor Authentication On EVERY Cloud Account
- Use a separate administrative account to manage your Cloud Services
- Build a process to maintain a Secure Configuration
- Build a process to remove permissions when someone leaves or changes roles
- Restrict access to your Cloud apps only from trusted devices
- Don’t use the same password or variants – Use a Password Management tool like LastPass
- Monitor your Cloud Service event logs
Questions???

Matthew A. Titcombe
CEO & Sr. Information Security Consultant
M.Titcombe@PeakInfoSec.com
https://www.linkedin.com/in/matthewtitcombe