Take it to the Cloud: The Evolution of Security Architecture

Dana Elizabeth Wolf
Head of Products, OpenDNS
OpenDNS/Cisco
@dayowolf
Critical Infrastructure

Desktops

Business Apps
When we talk about cloud security...

Virtual Appliances Hosted in Cloud

Security Delivered in Cloud

Security for New Architecture
<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2013</th>
<th>2015</th>
<th>Top Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>1</td>
<td></td>
<td>Data Breaches</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>2</td>
<td></td>
<td>Data Loss</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>3</td>
<td></td>
<td>Account Hijacking</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>4</td>
<td></td>
<td>Insecure Interfaces and APIs</td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td>5</td>
<td></td>
<td>Denial of Service (DoS)</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>6</td>
<td></td>
<td>Malicious Insiders</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>7</td>
<td></td>
<td>Abuse of cloud services</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>8</td>
<td></td>
<td>Insufficient Due Diligence</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>9</td>
<td></td>
<td>Shared technology vulnerabilities</td>
</tr>
</tbody>
</table>
#1&2 Data Breach/Data Loss

- **What is it?**
  - Data in the cloud that is exposed, lost or inaccessible

- **New Vectors for Data Breach**
  - Multi-Tenant Architecture Flaws in databases

- **Data Loss is similar, but exacerbated**
  - Secure Tunnel != Protection of Data
  - Losing encryption key
  - Offline backups
#3 Account Hijacking

- **What is it?**
  - Access to user identity & associated accounts

- **How have attacks changed?**
  - Reuse of credentials/passwords amplifies impacts of attacks
  - Man-In-The-Cloud stealing copy of synchronization token
#4 Insecure APIs

- What is it about?
  - APIs enables cross-cloud compatibility

- What are API attacks?
  - Kardashian Website Security Issues
  - The Buffer attack – due to improper OAUTH code
#5 Denial of Service (DoS)

What is it about?
- An attempt to make a machine or network resource unavailable to its intended users

How have attacks changed?
- Frequency: attacks per month on the rise
- Collateral Damage
- Size: Largest attack in 2004 was 8 Gbps. Now upwards of 400 Gbps
- Complexity: multi-vector attacks are becoming more common
#6 Malicious Insiders

- **What is it?**
  - A threat to the organization that originates from people within the organization such as employees, contractors, etc..

- **How have attacks changed?**
  - Amplified for cloud services due to convergence of IT Services/customers under a single management domain
  - Management of Identity once an individual leaves the organization
Insufficient Due Diligence

- **What is it?**
  - Investigation into a CSP prior to signing a contract. Clarity on SLAs

- **Why does it matter?**
  - You are now more dependent on another provider for success of your business
  - Added complexity of auditing multiple vendors’ security
  - Where cloud data resides, different laws apply
Solutions
Visibility

- Problems you want to solve
  - What Cloud Applications are being used across my enterprise?
  - What type of communication is happening to sanctioned & unsanctioned applications
  - How risky are the cloud applications being used?

- Who does it?
  - Secure Web Gateways
  - Cloud Access Security Brokers (CASB)
  - Next-Generation Firewall (NGFW)
Encryption / Data Loss Prevention (DLP)
Making a comeback?

- Problems you want to solve
  - Secure my data & reduce impact of data breach
  - Reduce impact data loss

- What do I need?
  - Use SSL
  - Encryption / Tokenization / Key Management
  - Apply DLP policies for Cloud Applications
  - Governance – Retention policy
Watching the User

- Problems you want to solve
  - Trust that proper controls are in place (CSP)
  - Prevent misuse of admin / employee accounts

- What do I need?
  - Identity Management
  - Access Management (audit trail, time-bound access, request for access)
  - User Entity Behavior Analytics
DDoS protection – who does it better?

- Problems you want to solve
  - Service stay up and running during a DoS or DDoS attack

- What do I need?
  - Leverage cloud architecture!
  - Absorption and mitigation of DDoS attacks
Problems you want to solve
- Higher confidence level in the CSPs security posture
- Incorporate CSPs SLAs and security processes into main IT process
- Protection

What do I need?
- Ask the CSP to share their internal security processes or assessment/audit
- Legally bind them to assessments. Review/negotiate indemnification clause.
- Review all SLAs
- Review of Architecture – look for APIs
In Review
Apply What You Have Learned Today

Next week you should:
- Identify sanctioned and unsanctioned applications in your company

In the first three months following this presentation you should:
- Understand cloud administrative accounts & monitor them
- Review if/where critical company data resides in the cloud
- Review existing legal contracts with CSPs to understand SLAs

Within six months you should:
- Identify new processes to put in place to integrate CSP security with internal security workflow
- Identify new key technologies for protection of cloud assets
Questions?