The Notorious 9
Cloud computing Threats

Moshe Ferber, CCSK
Onlinecloudsec.com
About

✓ Moshe Ferber, 39, Based in Israel
✓ Information security professional for over 20 years
✓ Founded Cloud7, Managed Security Services provider (currently owned by Matrix LTD)
✓ Partner at Clarisite – Your customer’s eye view
✓ Partner at FortyCloud – Make your public cloud private
✓ Member of the board at Macshava Tova – Narrowing societal gaps
✓ Certified CCSK instructor for the Cloud Security Alliance.
✓ Co-Chairman of the Board, Cloud Security Alliance, Israeli Chapter
What we are going to talk about

Cloud computing threats –
what they are?
how do they reflect in the real world?
What are the attacks vectors?

Sources:
✓ Cloud Security Alliance Notorious nine cloud computing threats.
✓ Cloud Security Alliance Cloud Computing Vulnerability Incidents: A Statistical Overview
Cloud computing 2014 – what affects security?

Consolidation will continue at IaaS level.
More supply Chain Attacks

Target Hackers Broke in Via HVAC Company

Metasploit’s DNS Registrar Hacked Via Fax

Intrepid Hackers Use Chinese Take-Away Menu To Access Major Oil Company
The Cloud & Cyber

Cloud Services
Ransom Malwares

Pay or Lose All Your Data!

Stealing CPU time

Crimeware-as-a-Service
✓ Cloud Provider will continue to be a target for data breaches, sometimes just for the accounts and not even for the data.
✓ iCloud, Evernote, Adobe tells the story well.
✓ But not all data lost happens due to hacking, Unintended disclosure is also happening.
✓ Cloud Computing and Shadow IT contribute to this phenomena.

Source: Verizon data breach report 2013
#2 Data Lost

- Hacking or simple failures – it does not really matter.
- Multi Cloud backup or external backups are not a “nice to have”.

Utility Computing provider Flexiscale’s Cloud appears to have floated away.

**Murder in the Amazon cloud**

Microsoft 'sorry' as Hotmail bug hits 17,000

Gmail users howl in anguish at 'disappeared' accounts

How Apple and Amazon Security Flaws Led to My Epic Hacking
New account Hijacking Motivation:

US MARSHALS MISTAKE CAUSES BITCOIN FUND TO LOSE 100 BTC
#3 Account Hijacking

- Most attacks used spear phishing.
- DNS ownership is also at attack vector
- Two factor & pro-active defenses for identifying account hijacking will continue.
- We will see more attacks on PaaS and on federation protocols.

"...the basic methods of gaining access to a victim’s environment are not. The most prolific is the old faithful: spear phishing. “

Verizon data breach report 2014

Zeus bot found using Amazon's EC2 as C&C server
#4 Insecure Interfaces and API’s

The cloud providers management dashboard, especially in IaaS, is the most intimidating attack vector.

For the second time this year, someone has broken into Twitter’s internal admin system and accessed accounts.

Why the Attack on Buffer Was a Serious Wake-Up Call for the Web

OPENSSL HACKERS USED WEAK PASSWORD AT WEB HOST TO DEFACE SITE

TOP THREAT RANKING

2 2010
4 2013

ONLINECLOUDSEC.COM
#5 Denial of Service

- Network DDOS are becoming less common when talking about cloud providers.
- But application level attacks are increasing.

Cybercrooks use DDoS attacks to mask theft of banks' millions

WikiLeaks hit by second DDoS

DDoS attack against Bitbucket darkens Amazon cloud

DNS Flood DDoS Attack
90 Million requests/sec (Above 110 Gbps)
#6 Malicious Insider

**GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated)**

Fired techie created virtual chaos at pharma company

Entire kids TV show deleted as former data hosting employee takes revenge

Microsoft accuses former employee of cloud data theft
#7 Abuse of Cloud Services

U.S. based Cloud Hosting providers contribute 44% of Malware distribution

Twitter transformed into botnet command channel

PlayStation Network hack launched from Amazon EC2
Cloud economics strikes again

Sudden FBI Raid claims Innocent Web Server – Is Your Website Next?

Attackers Using Dropbox and Wordpress to Target, Disguise and Distribute

Megaupload user content safe for two more weeks
EFF joins battle to free user data from shuttered company’s servers
#8 Insufficient due Diligence

- Evaluating your provider is hard, very hard.
- Government legislation and industry efforts will lead to better understanding of Cloud Accountability.
- CSA will help in promoting transparency and provider evaluation methodology.

Eli Lilly dumps Amazon Web Services over legal struggle

Nirvanix cloud customers face worst nightmares

You have 2 weeks to pickup your cloud
#9 Shared Technologies vulnerabilities

Zoho users logging into other accounts by accident

Windows Live suffers user details identity crisis

Cloud file-hosting service Dropbox leaves 25m users' accounts unlocked for four hours

New Virtualization Vulnerability Allows Escape To Hypervisor Attacks
From the infrastructure point of view SDN might solve some of the problems.

Innovation is required on the application layer, Identity Management and encryption.

IBM gets patent to battle cloud ‘noisy neighbor’ problem with SDN
## Cloud Vulnerability Incidents
### A Statistical Overview

<table>
<thead>
<tr>
<th>#</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Abuse of cloud services</td>
</tr>
<tr>
<td>T2</td>
<td>Insecure Interfaces and API</td>
</tr>
<tr>
<td>T3</td>
<td>Malicious Insiders</td>
</tr>
<tr>
<td>T4</td>
<td>Shared Technologies Vulnerabilities</td>
</tr>
<tr>
<td>T5</td>
<td>Data Loss</td>
</tr>
<tr>
<td>T6</td>
<td>Account Hijacking</td>
</tr>
<tr>
<td>T7</td>
<td>Insufficient due diligence</td>
</tr>
<tr>
<td>T8</td>
<td>Hardware failures</td>
</tr>
<tr>
<td>T9</td>
<td>Nature disasters</td>
</tr>
<tr>
<td>T10</td>
<td>Closure of cloud services</td>
</tr>
<tr>
<td>T11</td>
<td>Cloud Related Malware</td>
</tr>
<tr>
<td>T12</td>
<td>Inadequate infrastructure design and planning</td>
</tr>
</tbody>
</table>

![Number of Cloud Vulnerability Incidents by threat category](image-url)
Invest in consumer visible controls.

You might be a chain in supply chain attacks - Think about your role in your customers security.

Start with good building block:

- Secure Software development life cycle.
- Security in operations.
- Transparency.

CSA tools and research can help you achieving good foundations.
Recommendation, Cloud Consumers

- Invest in education.
- There are 4 kinds of security controls. Make sure you use the right mixture.
- Establish Cloud Strategy.
- Audit your provider, his services, and the supply chain.

Preventive
- Anti virus
- Authentication

Detective
- IDS
- Logs

Corrective
- Patches
- Scanning

Compensatory
- DR & backups
- Audits
Questions?

Moshe Ferber
- moshe@onlinecloudsec.com
- +972-52-8342313
- www.onlinecloudsec.com

http://www.linkedin.com/pub/moshe-ferber/0/58a/828
KEEP IN TOUCH

Moshe Ferber

📧 moshe@onlinecloudsec.com
📞 +972-52-8342313
🌐 www.onlinecloudsec.com

http://www.linkedin.com/pub/moshe-ferber/0/58a/828

Cloud Security Course Schedule can be find at:
http://www.onlinecloudsec.com/course-schedule