Risk and Reward: A cloud user perspective

Faud Khan: TwelveDot/Industry Canada

Topics

- User Profile
- Background
- Key Risk Factors
- Privacy
- What is not being provided
- What is needed

User Profile

- AKA Cloud User
- Large/Medium Enterprise
- 1000+ employees
- Will have +1 data centers typically more globally
- Key aspects of operation
  - Operational costs
  - Security
  - Privacy
  - Local Regulatory Compliance

Background

- Over the past 3 years working with the following companies:
  - Cloud Service Providers {CSP}
  - Carriers
  - Large/Medium Enterprise
- Lots of the experience learned in these environments was provided as comments towards ISO/IEC 27017
- One of the large enterprise currently has a “No” cloud policy
  - Over 100K employees in 40 countries
  - 6 global data centers
- Why would this kind company not want to consider cloud?

Key Risk Factors

- Fear
  - Who owns my data/IP?
  - Will a foreign government take my data and what will they do with it?
  - If the provider is compromised will I be notified?
  - If the provider experiences an outage how am I able to operate?
- Some of these fears are justified
  - See the Google request for data site?
  - Major outages on cloud provider networks
  - What happened to the organizations who depended on these?
    - No public facing web presence
    - Employees were not able to work {0 productivity == 0 $$$$}

Privacy

- Cross border data transfer {*risk teams dread this*}
- Need better controls for authentication and identification of users
- Governments request for data
- Compliance to regulatory requirements
- Data retention and destruction
- Notifications of privacy breach

What is not being provided

- Security policies (data disclosure, privacy, incident handling)
- Certifications or standards used for operations {anything}
- A CSO or equivalent who actually knows security
- Ability to perform risk assessments against the infrastructure
  - Dependent on architecture of CSP
- Detailed Metrics/Notifications
  - Outages
  - Metrics – network, access, servers, authentication
  - Raw logs – reporting

What is needed

- Vendors need to stop confusing customers with irrelevant terms – Get rid of the misconceptions of what the cloud is and it can offer
- In some countries governments need to provide some guidance to vendors and enterprise on what the key aspects of cloud computing should be
- Reference models based on standards
- Common terminology

Final Thoughts

- Mobile will complicate matters {data is available everywhere}
- Mobile standards for security/cloud are needed
- Need a common measurement standard for operations
  - 27017, CSA, NIST
  - SAS70s just don’t cut it for cloud!
- A security vulnerability registry against cloud technologies
  - New aspect of CVE???
- CSPs need to be open, willing and prepared to deal with these questions

Thank-You

Questions???

About Me

- 17 years industry expertise in carrier and enterprise security
- Currently principle at TwelveDot Inc.
- Focus on Mobile, Cloud and Smart Grid security
- 1 patent granted and 9 pending
- Chair of CAC-ITS in Canada (mirror committee to ISO/IEC SC27 Information Technology Security)
- Member of Cloud Security Alliance (Active on Telecom Working Group and Standards Council)
  - Currently liaison to CAC-ITS for CSA.