Security Architecture
- Week 13 -

Cloud Security

Week 13

- In the News
- Week 13 assignment
- Lecture: Cloud Security
- Quiz
- Final Project Briefing and Discussions

In the News

Week 13 Assignment

Cloud Security

As mobile devices such as smart phones and tablet computers increasing displace desktop computers and laptops in both business and personal use, protecting mobile computing is the becoming an essential component in privacy and the protection of business information assets.

Cloud Security

- What do we mean by cloud security?
- 9 Top Threats
- Vendor Management
- Compliance (standards)
- Auditability
- Security Architecture
- Securing your data
- Physical security
- Business risk
- Architecture Options
- Top 9 Threat Mitigations

Cloud Security

What do we mean by the cloud?

- Web storage
- Platform as a service (PaaS)
- Software as a service
- Business Process Outsourcing

9 Top Cloud Computing Threats

1. Data Breaches
2. Data Loss
3. Account or Service Traffic Hijacking
4. Insecure interfaces and APIs
5. Denial-of-service
6. Malicious Insiders
7. Cloud Abuse
8. Insufficient Due Diligence
9. Shared Technology Vulnerabilities

Vendor Management

- Who should you trust with your data?
- Your day-to-day business operations?
- Vendor comparisons
- Reputation
- Background Checks
- Cost versus Risk
- Insurance
- Contract
- Service Level Agreement
- Penalties for non-compliance
- Impact of risks

Compliance

- General standards for data center management
- Local ordinances
- Industry specific requirements (PCIDSS/HIPPA)
- Security standards
- Architectural standards

Auditability

- Monitoring
- Standard Reporting
- Availability of direct access and review
- Financial Audits
- IT Audits
- Involvement of your internal audit team
- Security Audits
- Certifications

Security Architecture

- Industry best practices
- Identity management
- Access management
- Data Protections
- Intrusion Detections
- Monitoring and Surveillance
- Employee screening
- Multi-tenant security
- Backup and resiliency strategy
- Physical security

Securing Data

- Data Architecture
- Access Controls
- Multi-tenancy issues
- Data masking and encryptions
- Privacy considerations
- Backup and Recovery

Physical Security

- Location
- Physical layout / Lighting
- Alarms – including fire, intrusion, tamper, motion
- Physical barriers – including fences, bollards, tire strips, gates
- Access points – including doors, gates, turnstiles, windows, docks, elevators and
- Guards
- Monitoring/CCTV
- Access methods – including locks, proximity cards/swipe cards, code or cipher locks

Business Risk

- Loss of direct control
- Loss of business knowledge
- Vendor failure to deliver
- Scope creep
- Cultural Issues
- Loss of key personnel

Architecture Options

- Ref architecture
- Local resiliency
- 3rd party resiliency
- Hybrid cloud
- Shared DLP, IDS management
- Local cloud

9 Top Cloud Threat Mitigations

1. Data breaches – credentials management and access controls
2. Data Loss - shared DLP/IDS management monitoring
3. Account or service traffic hijacking – network security, proactive network analytics
4. Insecure interfaces and APIs - application and patch management, machine land user level policy enforcement
5. Denial of service – sub-netting, DMZ construction, load balancing , DDOS detection software appliance

9 Top Cloud Threat Mitigations (Cont.)

6. Malicious insiders – background checks, DLP, activity monitoring, behavioral analytics
7. Cloud abuse – activity monitoring, behavioral analytics
8. Insufficient Due Diligence – Vendor management, background checks, resiliency strategies
9. Shared technology vulnerabilities – VM instance management, patch management, shared security administration, behavioral analytics

Week 13 (14) Quiz

Final Project