CLOUD SECURITY AND DATA PROTECTION

Informationstechnisches Kolloquium

Thomas Lorünser
Center for Digital Safety & Security
THE PROBLEMS WE ARE FACING

• Complexity of IT-systems is increasing:
  • Moon landing with 7.500 lines of code (LoC)

• Systems are more connected
  • Internet-of-Things (IoT), “always-on”, pervasive comp.
  • Machine-to-Machine (M2M) communication
  • Virtual infrastructures (Cloud), etc.

• Industries are trending towards open network infrastructures
  • Open protocols (e.g. All over IP)
  • Involving more stakeholders connecting more systems

• Dependency on ICT systems is dramatically increasing
  • Smart grid, smart home, smart cities, smart manufacturing
  • eGovernment, eHealth, eBusiness, Mobile payment
MEGATRENDS INFLUENCING OUR WORLD

• Some Socio-Economical Megatrends
  • Demographics and consumption
  • Global competition and innovation
  • All-round sustainability

• Some ICT Megatrends
  • Dynamic collaboration (Social media, Web 2.0, Cloud)
  • Mobility and ubiquitous connectivity
  • Data mining and business intelligence (Big Data)
  • Computing paradigms (Cloud)
  • Real-world connectivity (seamless and bi-directional interaction on a global scale)
POTENTIAL OF CLOUD COMPUTING

- EU expect a net annual gain of €160 billion to EU GDP by 2020 (or a total gain of nearly €600 billion between 2015 and 2020) with strategy
- EU expect to see 3.8 million jobs generated following full implementation of the strategy
- Fields for cloud computing:
  - Business
  - Private
  - Public
  - Research & Development
- Help to protect environment (green IT)
- They are a great chance for SME (99% SME in EU)
CLOUD ADOPTION BARRIERS

Cloud Adoption Barriers

#1
53%
General security risks

#2
42%
Legal & regulatory compliance

#3
40%
Data loss & leakage risks

#4
35%
Integration with existing IT environments

#5
26%
Lack of expertise

↑ 8% p.p. from last year
↑ 13% p.p. from last year
↓ 1% p.p. from last year
↑ 6% p.p. from last year
↑ 10% p.p. from last year

Loss of control 23% | Management complexity 20% | Increased agility 28% | Fear of vendor lock-in 18% | Internal resistance and inertia 18% | Lack of staff resources 17% | Lack of transparency and visibility 15% | Lack of maturity of cloud service models 14% | Cost/Lack of ROI 13% | Lack of budget 13% | Performance of apps in the cloud 12% | Lack of management buy-in 10% | Lack of customizability 9% | None 9% | Dissatisfaction with cloud service offerings/performance/pricing 7% | Billing & tracking issues 7% | Lack of support by cloud provider 6% | Availability 5% | Not sure/Other 10%

Source: (ISC)² - 2016 Spotlight on Cloud Security Report
WHAT IS THE CLOUD – A SECURITY STANDPOINT?

There is no new technology involved, it is about the way the resources are delivered:

- On-demand (self-)service
- Over the network
- In an elastic way (provisioning)
- Resource pooling (virtualization)
- Measured service (optimized)

Source: http://www.bradnash.com
WHAT IS GOING ON IN THE DATA CENTER?

WHAT IS GOING ON IN THE DATA CENTER?

CLOUD SECURITY CONCERNS

- Data loss/leakage: 49%
- Data privacy: 46%
- Confidentiality: 42%
- Legal and regulatory compliance: 39%

Data sovereignty/control 34% | Accidental exposure of credentials 26% | Lack of forensic data 26% | Incident & problem management 25%
Visibility & transparency 19% | Availability of services, systems and data 17% | Liability 17% | Disaster recovery 13% | Performance 13% | Business continuity 13% | Fraud (e.g. account hijacking) 12% | Not sure/Other 5% | None 1%

Source: (ISC)² - 2016 Spotlight on Cloud Security Report
PROTECTING DATA IN THE CLOUD

Source: (ISC)²
PROTECTING DATA IN THE CLOUD

Dropbox: Oops, yeah, we didn't actually delete all your files – this bug kept them in the cloud
Biz apologizes after years-old data mysteriously reappears

GitLab.com melts down after wrong directory deleted, backups fail
Upstart said it had outgrown the cloud – now five out of five restore tools have failed

$3.2 Million HIPAA Fine: An Analysis
The Reasons Behind OCR's Tough Penalty in Case Against Children's Medical Center of Dallas

Google Cloud Outage: Virtual Networking Breakdown
Google's virtual networking software stopped providing routing updates, and customers lost their connections to the outside world.
Amazon S3-izure cause: Half the web vanished because an AWS bod fat-fingered a command

Basically, Team Bezos pulled a GitLab
MOST EFFECTIVE CLOUD SECURITY TECHNOLOGIES

65%  Data encryption

57%  Network encryption

48%  Intrusion detection & prevention

Trained cloud security professionals 45%  |  Access control (e.g. CASB / Cloud Access Security Brokers) 45%  |  Log management and analytics 43%  |  Firewalls / NAC 40%  |  Data leakage prevention 40%  |  Endpoint security controls 40%  |  Patch management 38%  |  Network monitoring 37%  |  Single sign-on / user authentication 35%  |  Anti-virus / Anti-malware 35%  |  Employee usage monitoring 29%  |  Mobile device management (MDM) 25%  |  Database scanning and monitoring 24%  |  Content filtering 24%  |  Security Information and Event Management (SIEM) 22%  |  Cyber forensics 21%  |  Not sure/Other 12%

Source: (ISC)² - 2016 Spotlight on Cloud Security Report
CURRENT SITUATION IN THE CLOUD
TRUSTWORTHY CLOUD COMPUTING
CLOUD COMPUTING CERTIFICATIONS

- Cloud Security Alliance (OCF Level 1,2,3)
- EuroCloud (Start Audit)
- ISO / IEC 270xx (JTC1 / SC27, SC38)
- PCI (Payment Card Industry)
- AICPA (SOC 1,2,3)
- TÜV Reihnland
- …
SECURITY BENEFITS OF CLOUD

- Benefits of scale
  - Multiple locations
  - Edge networks
  - Improved timeliness and response
  - Threat management
- Security as a market differentiator
- Standardized interfaces for lower layer services
- Rapid, smart scaling of resources for security services (DDoS)
- Audit and evidence gathering
- More timely and effective and efficient updates and defaults
- Audits and SLAs force better risk management
HOW TO ADOPT TO CLOUD

- Develop a cloud strategy
- Develop security requirements and policy
- Definition of services/interfaces/responsibilities
- Prepare migration and usage
- Security concept
- Selection of cloud provider
- Migration and operation
- Termination

Source: BSI: Secure use of cloud services
MAYOR TOPICS FOR CLOUD SECURITY

• Enable transparency
• Clear separation of responsibilities
• Standardization and open standards
• Compliance to data protection and privacy regulation
NEW RELEVANT REGULATIONS?

GDPR:
- Extended scope (applies to data processors)
- Extended responsibilities and accountability
- Explicit valid consent
- Immediate data breach notifications
- Possible sanctions have been raised
- Right to erasure
- Data portability
- Privacy by design

Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life.

08.05.2017
WHAT ABOUT PRIVACY?

GDPR vs. Big Data Strategy
BIG (TECHNOLOGICAL) CHALLENGES IN PRIVACY

• How to implement it right
• Empower the user to enforce his rights
• Enforce data privacy on a technical level
• Meta-data privacy for best protection
• Unlinkability in large-scale networked sys
• Develop new PETs allowing to improve GDPR enforcement
• Co-exist with the need for IoT applications, still enable reasonable sharing

Better privacy enhancing technologies for for cloud, IoT and smart applications
PRIVACY BY DESIGN

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric