Jan Philipp
Manager, Cyber Risk Services
Enterprise Architect

Security Challenges of Cloud Providers
("Wie baue ich sichere Luftschlösser in den Wolken")

Introduction

  » Who I am (http://archimatrix.com/jphilipp)
    Gh0st, Sanity Gambit, Unit-Y, ….

  » Why this topic:
    Security Challenges of Cloud Providers

Background Info

  » What are Clouds and what can they do

  » What Cloud security information already exists

Purpose today

Agenda

» Cloud Challenges

Targeted and opportunistic attacks against Cloud and
EDCs

» Security models, frameworks and white papers

NIST, BSI, and ENISA – putting it all together

» Explanations of the risks categories

What goes where & what is different in the cloud

» Working best practices from the field

What all the existing tools don't adequately address

» "All that matters is results;
I don't care how it's done"

» "I don't want to own assets — I want
to pay for elastic usage, like a utility"

» "I want accessibility from anywhere,
from any device"

» "It's about economies of scale, with
effective and dynamic sharing"

Acquisition Model
Service

Business Model
Pay for usage

Access Model
Internet

Technical Model
**Scalable, elastic,
shareable**

Cloud Computing:

A style of computing where massively scalable IT-enabled capabilities
are provided "as a service" to external customers using Internet
technologies

Similarities

» Sets of interfaces and infrastructure

» Extensible, solutions built on platform, platform hides infrastructure

» Multiple levels of platforms possible

» Platform as "you are here" Value determined by what is made accessible

» Similar success factors (ecosystem)

Differences

» Not a stand-alone platform that is always purchased

» Separated by a network (the Internet)

» Not a client server platform, but a distributed platform - WOA

» Access to data and capabilities as a result of community

» Global-class and elastic Consumer-inspired

Cloud Challenges (Tech)

Costs
Economies of scale limits, or customer trades data or advertising for services

Scalability
Parallel processing, no problem; sequential processing, different story

Service Management
Technologies immature

Connection
Only as good as the Internet, unless you pay to "harden" your connection

Culture
Trust, chargeback, sharing

Customization Difficult.
At least with monolithic applications
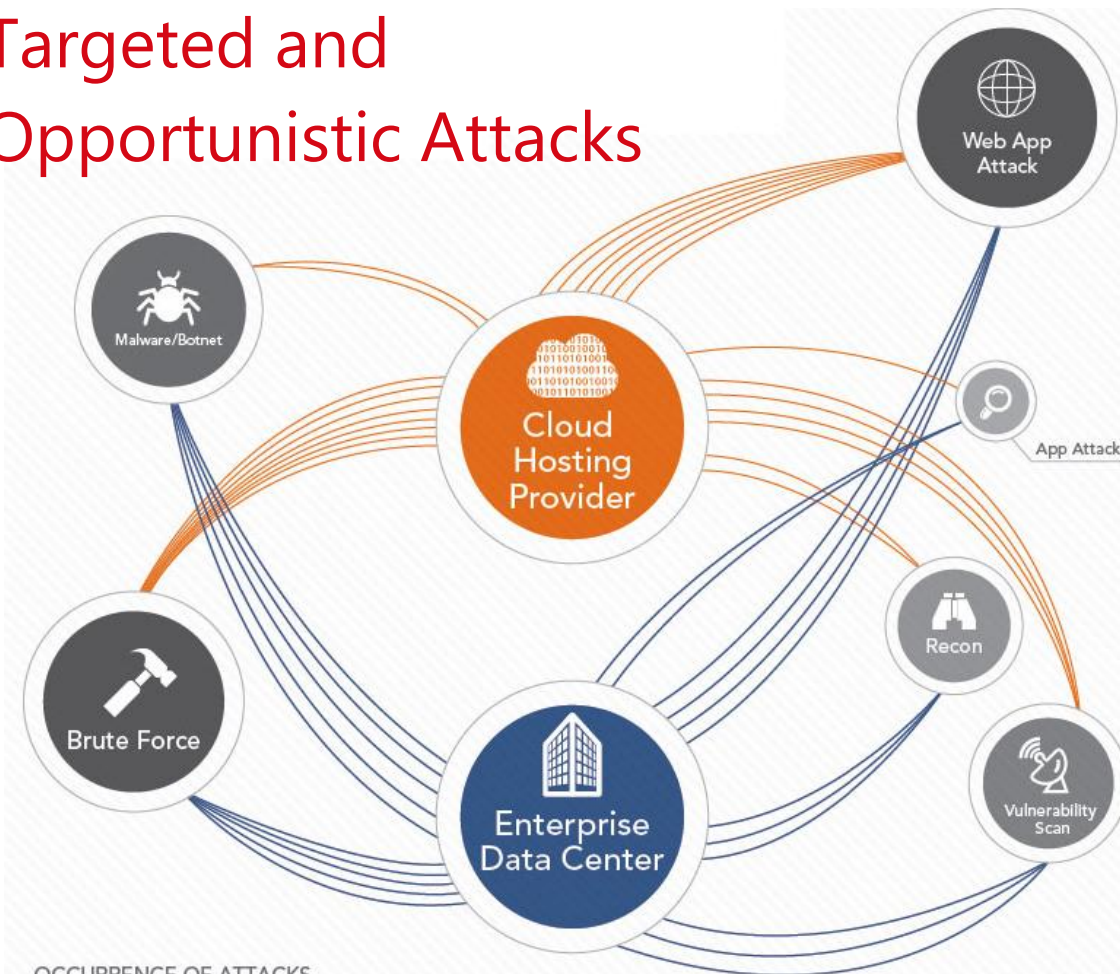
High Availability
Stateless, no problem; stateful, same issue as in enterprises

EC2 & S3

Adapted from: Gartner Summit Event

6

Targeted and Opportunistic Attacks

Source: AlertLogic
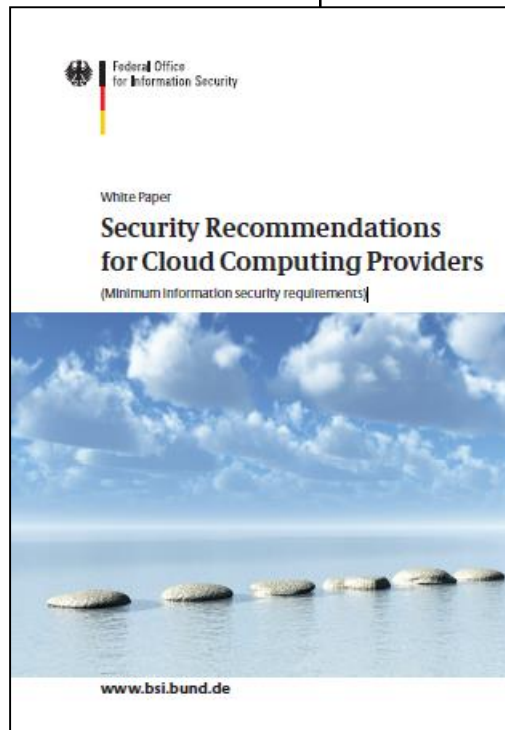2013 State of Cloud Security Report

ENISA (European Network and Information Security Agency)

**Cloud Computing
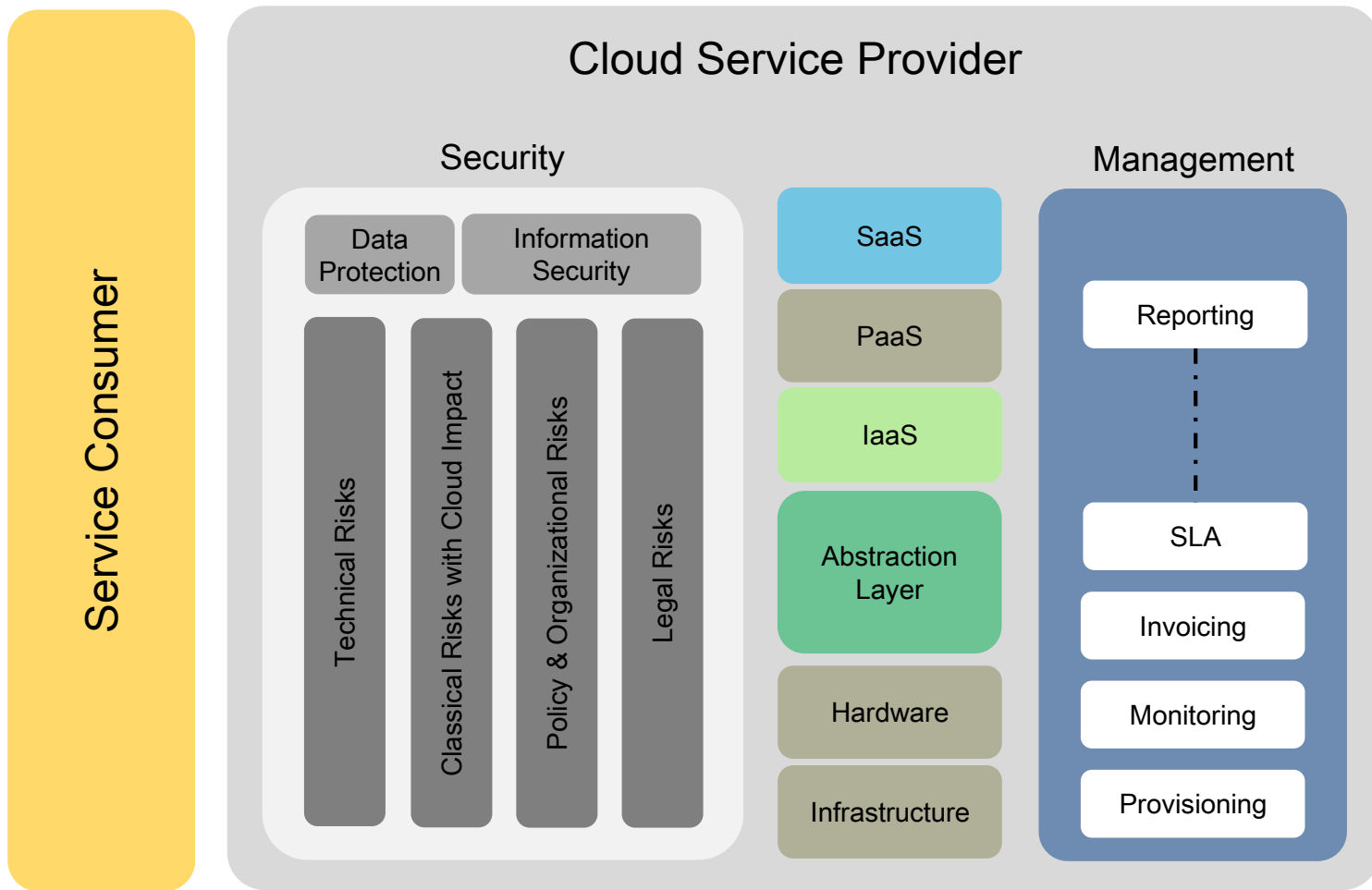Benefits, risks and recommendations
for information security**
Original Nov 2009, Updated Dec 2012

BSI (federal Office of Information Security)

***Security Recommendations
for Cloud Computing Providers***
June 2011

NIST (National Institute of Standards and Technology)

All compliant with the *Nov 2013*
**NIST Cloud Computing 5
Security Reference Architecture**

General risks

> » Provider solution lock-in

> » Loss of governance

> » Compliance challenges

Event driven risks

> » Cloud service termination or failure

> » Cloud provider acquisition

> » Loss of business reputation due to co-tenant activities

> » Supply chain failure
> (due to Cloud provider outsourcing specialized tasks to 3rd parties)

Confidentiality

- » Isolation failure
- » Data leakage
  On up/download, intra-cloud, interception in transit
- » Insecure or ineffective deletion of data

Integrity

- » Cloud provider malicious insider (abuse of high privilege roles)
- » Undertaking malicious probes or scans

Availability

- » Loss of encryption keys
- » Resource exhaustion and denial of service DDoS/EDoS
- » Conflicts: Customer hardening vs. cloud environment
- » Compromise service engine

General legal risks

- » Subpoena and e-discovery
- » Risk from change of jurisdiction
- » Export controls
- » Data protection risks

Additional legal considerations

- » "Bundesdatenschutz" (BDSG)
- » Information Security (ISO27001)
- » Governance (ISO38500)
- » Risk Management (MaRisk, KontraG)
- » Internal control systems (JAP) (IDW PS261, 330, ERS FAIT 1)
- » Outsourcing (PS951/SAS70//SSAE16, ISAE3402)

Confidentiality

» Privilege escalation

» Social engineering attacks, like impersonation

» Backups lost or stolen, or theft of computer equipment

Integrity

» Modifying of network traffic

» Loss or compromise of logs
(manipulation of forensic investigation)

Availability

» Network breaks

» Poor network management (congestion, mis-connection, ...)

» Natural disasters

» Transitions

Tips and Best Practices

From the Field

For

Cloud Providers

Policy & Organizational Risks

» Provide the
Security Architecture Drawing

» Allow Access to the Environment Log
and Systems

» Allow the Use of Correlation Tools and
Log Retention

» Have a Security Point Person to Serve
the Contractor During the Contract
Period

» Manage Vulnerabilities, Threats and
Risks by Aligning With the
Contractor/Tenant

» Have the SAS 70 Certification or Similar
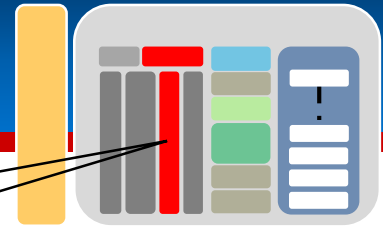
» Permit External Audits for Cloud
Security

Relevant Statements

Share information
between Cloud provider
and tenant/contractor

Be transparent as
provider.

Legal Risks

» Establish SLAs in the Contract, Including in the Cases of Security Incidents

» Detail the End of Business Operations Process in the Contract

» Detail the Process for Responding to Legal Requirements

» Identify Where the Solution Data Center(s) Will Be to Meet Local Legal Particularities

Relevant Statements

You have to think of everything both as cloud consumer and provider at the beginning!

You have to make provisions for all potential changes at the beginning.

Technical Risks

» Have Specialized Protections for the Perimeter

» Hold the Firewall Segregating All Networks, including Server Environment Operators and Users

» Segregate Functions Inside the Provider

» Detail How Much the Environment/Infrastructure Is Shared With Other Clients

» Notify How Information Leakage Control is Managed

» Detail Procedures in Case of DDoS Attacks

» Demonstrate the Process of Cryptographic Keys Management

Relevant Statements

Treat the cloud as your company perimeter – it's not just firewalls

Understand the other types of tenants hosted and how they are separated.

⛈ Sec: Best practices

Classic IT Risks with Cloud impact

» Allow Vulnerability Analysis and Ethical Hacking

» Share the Business Continuity Policy and Disaster Recovery Plan

» Detail the Data Disposal Process in the Contract

» Access Control with Strong (ideally multifactor) Authentication

Relevant Statements

Treat the security and access of Cloud applications like you would any other application.

Plan for disaster and change in the Cloud and include it in your plans.

Thanks for coming out!

Jan Philipp
Manager, Cyber Risk Services
"Cloud klaut" aber trotzdem

jphilipp@deloitte.de