Impressionen RSA (Security) Konferenz, Kalifornien, März

Security didn't kill the cloud

Martin Rutishauser

Group Security, Fachkader

Swisscom (Schweiz) AG

Rotkreuz, 27.08.2019

"Will Security Kill The Cloud?" – Forbes, 26. August 2014

Forbes

Billionaires Innovation Leadership Money Consumer Industry Life

4,233 views | Aug 26, 2014, 01:30pm

Will Security Kill The Cloud?

SungardAS Contributor Brand Contributor
SungardAS BRANDVOICE

By Sue Poremba

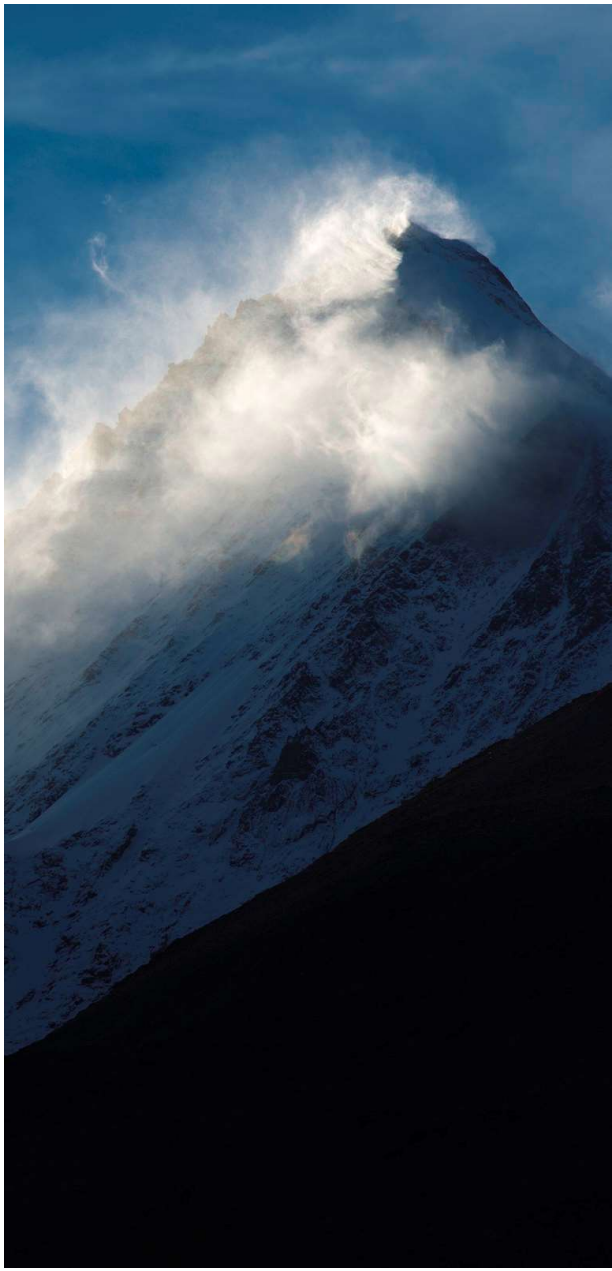
What's not to like about the cloud? It fits well into the way businesses operate today -- remotely, collaboratively, and globally. It also helps to get rid of one of computing's worst security threats: portable storage devices like thumb drives and hard drives that are easily lost or preloaded with malware.

Von Mythen und tatsächlichen Bedrohungen

If my data is in a public cloud, it's inherently unsafe
The thinking goes like this: Because I can't see it or touch it, others can steal it.

Public clouds are impenetrable
Nothing is impenetrable, including public clouds that have all of their security capabilities turned on.

The big vulnerability is the human factor
Users who share accounts, admins who write passwords on sticky notes, firewalls that are not updated, and all that sort of stuff. Although most security solutions are solid, the security operations are typically where companies fall down, both in the cloud and on-premises.



1. On-Premise to Cloud

Sourcing

Journey to Hybrid IT

2. Herausforderungen

Die grösste Hürde

Schutzziele, Compliance und Governance

Shared Responsibility Model

Security Architecture Domains

3. Massnahmen

Internes Verständnis schaffen

Evaluation Cloud Provider

4. Fazit

On-Premise to Cloud: Sourcing

Wohin sich der Schweizer Markt und die Unternehmen bewegen

10%

der Schweizer Unternehmen werden im Jahr 2020 noch auf den reinen internen IT-Betrieb setzen

20%

Der Firmen werden im 2020 Serverless Technologie einsetzen (5% Ende 2018).

50%

Der Schweizer Unternehmen planen ihre Rechenzentren vollständig in die Cloud zu schieben

Faktor 2

Fachkräftemangel in der Informatik liegt über dem Schweizer-Durchschnitt

>95%

Der in 2022 sich ereignenden IT Security Zwischenfälle auf der Cloud werden sich die Firmen selber zuschreiben müssen

On-Premise to Cloud: Journey to Hybrid IT – How To

Standards:
IT Grundschutz (BSI)
ISO 27001
Best Practices
…

ENTERPRISE On-Premise IT
Dediziertes IT Personal
IT-Sicherheitsmanagement
(Bereich aus der Informationssicherheit)
Wir kennen "Perimeter Security" und leben "Zoning"
Handlungsebenen: Governance, Risk & Compliance
COTS & traditionelle Software Entwicklung, manuelles Patching, usw

Datensicherheit versus Datenschutz

- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking
- Facility

Physische Sicherheit
Logische Sicherheit
Organisatorische Sicherheit

1. Business Strategie
2. ICT Strategie - make or buy / Roadmap

Primäre Treiber:
Innovation? Personalmangel? Kostendruck?

Sourcing anstatt Schatten-IT
Richtlinien (Bsp: Cloud Nutzung, "Smart Cloud" anstatt "Cloud First")
Definiere das "Hybrid IT Target Operating Model"
Achtung: Delegation von Aufgaben, aber nicht der Verantwortung!
Due Diligence zwingend
SLAs sind ein Schlüssel zum Erfolg
Migrationsstrategien (Bsp: Lift&Shift, Rearchitecture)

On-Premise to Cloud: Journey to Hybrid IT - a Cloud refresher

ENTERPRISE On-Premise IT

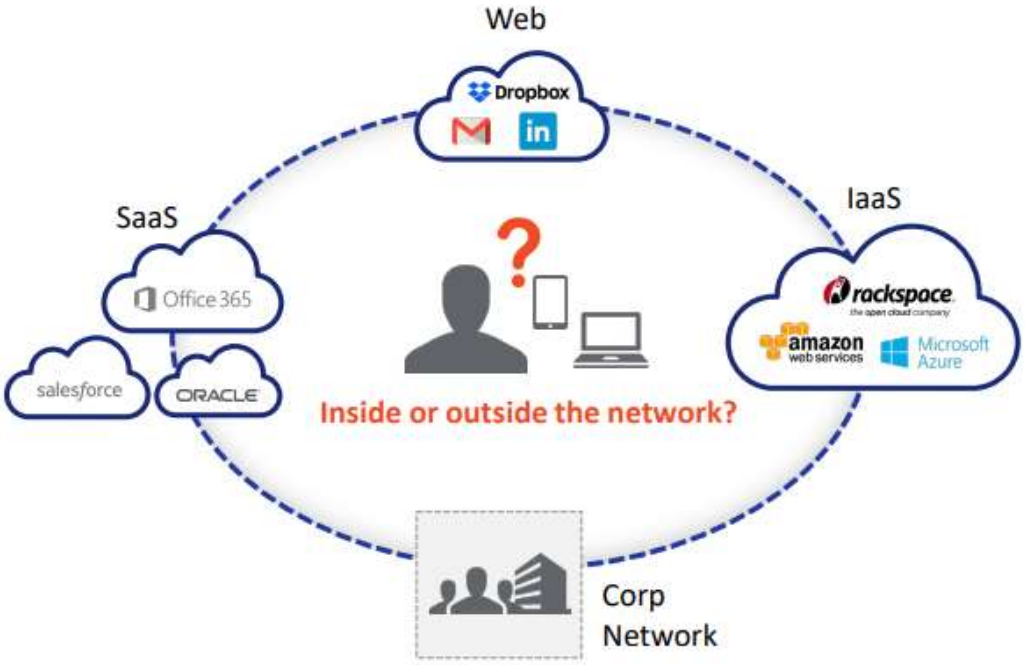
Cloud
Broad network access, rapid elasticity, measured service, on-demand self-service, resource pooling

Cloud Deploy-ment Models	**Cloud Service Models (XaaS)**	**Cloud Native**	**Backend Architectures**
Public Private Hybrid	IaaS, CaaS, PaaS, FaaS, DaaS, SaaS	Automatisierung, Portierbarkeit (OS), kein Server/OS management, Continuous Deployment, Scaling	Monolith Microservices Functions / Serverless

applications and services that automate and integrate the concepts of DevOps, continuous delivery, micro-services, and containers

On-Premise to Cloud: Journey to Hybrid IT – Zero Trust

In a world of cloud and mobile, what is the next network security blueprint?



The firewall is dead long live Zero Trust

Quelle: https://www.rsaconference.com/writable/presentations/file_upload/spo3-t08-how_to_apply_a_zero-trust_model_to_cloud_data_and_identity.pdf

1. On-Premise to Cloud

Sourcing

Journey to Hybrid IT

2. Herausforderungen

Die grösste Hürde

Schutzziele, Compliance und Governance

Shared Responsibility Model

Security Architecture Domains

3. Massnahmen

Internes Verständnis schaffen

Evaluation Cloud Provider

4. Fazit

Herausforderungen: die grösste Hürde

« The basic issue is, do I trust that other legal entity that has my data on their hard drive? »

Bruce Schneier
CTO at Co3 Systems In

Herausforderungen: Schutzziele, Compliance und Governance

Schutzziele der Informationssicherheit

availability, integrity, confidentiality **(AIC triad)**

authenticity, non repudiation, accountability, … **(weitere)**

Unternehmenshandlungsebene "Compliance"

Legislatur: Datenschutzgesetz CH, Datenschutzbehörden, EU-DSGVO / GDPR, Cloud Act, …

Standards: ISAE 3402, ISO27001, …

Industriespezifika: FINMAG / Rundschreiben, PCI DSS, …

…

Unternehmenshandlungsebene "Governance"

Interne Cloud Nutzungsweisungen

IT Grundschutz (BSI)

ISF Information Security Form - Standard of Good Practice

CSA Cloud Security Alliance – Security Controls

CSCC Cloud Standards Customer Council – vendor-neutral guidance

…

Herausforderungen: Shared Responsibility Model

Das Modell erlaubt eine strukturierte Cloud Security Diskussion, um als Kunde

a) eine realistische Erwartungshaltung gegenüber Cloud Providern zu entwickeln

b) zu verstehen was die eigenen Aufgaben und Pflichten sind

Customer managed

Provider managed

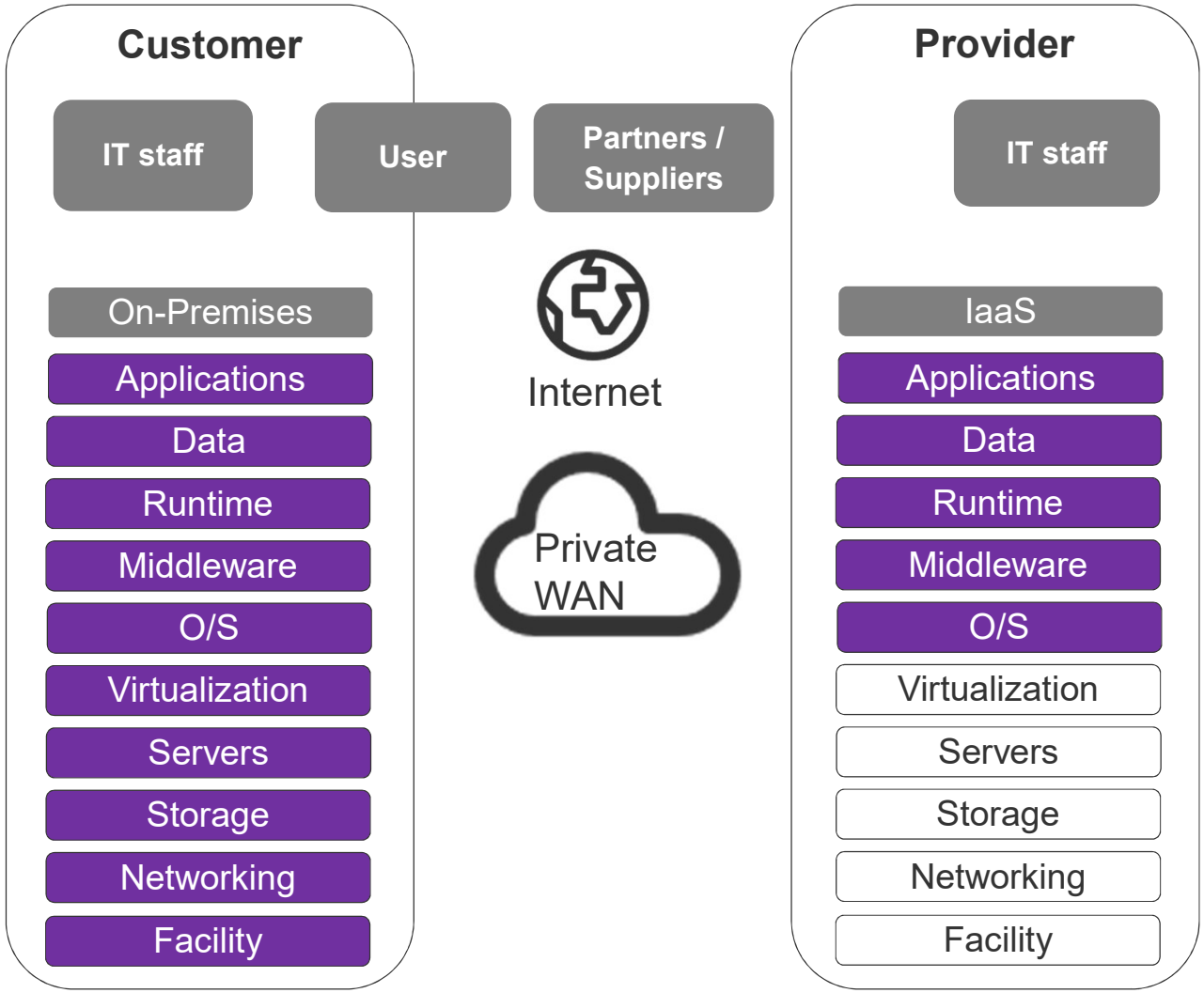
Fertigungstiefe = was produziere ich intern, was übergebe ich einem Dienstleister/Provider?

On-Premises	IaaS	CaaS	PaaS	SaaS
Applications	Applications	Applications	Applications	Applications
Data	Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Containers	Middleware	Middleware
O/S	O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking	Networking
Facility	Facility	Facility	Facility	Facility

Herausforderungen: Security Architecture Domains - Übersicht

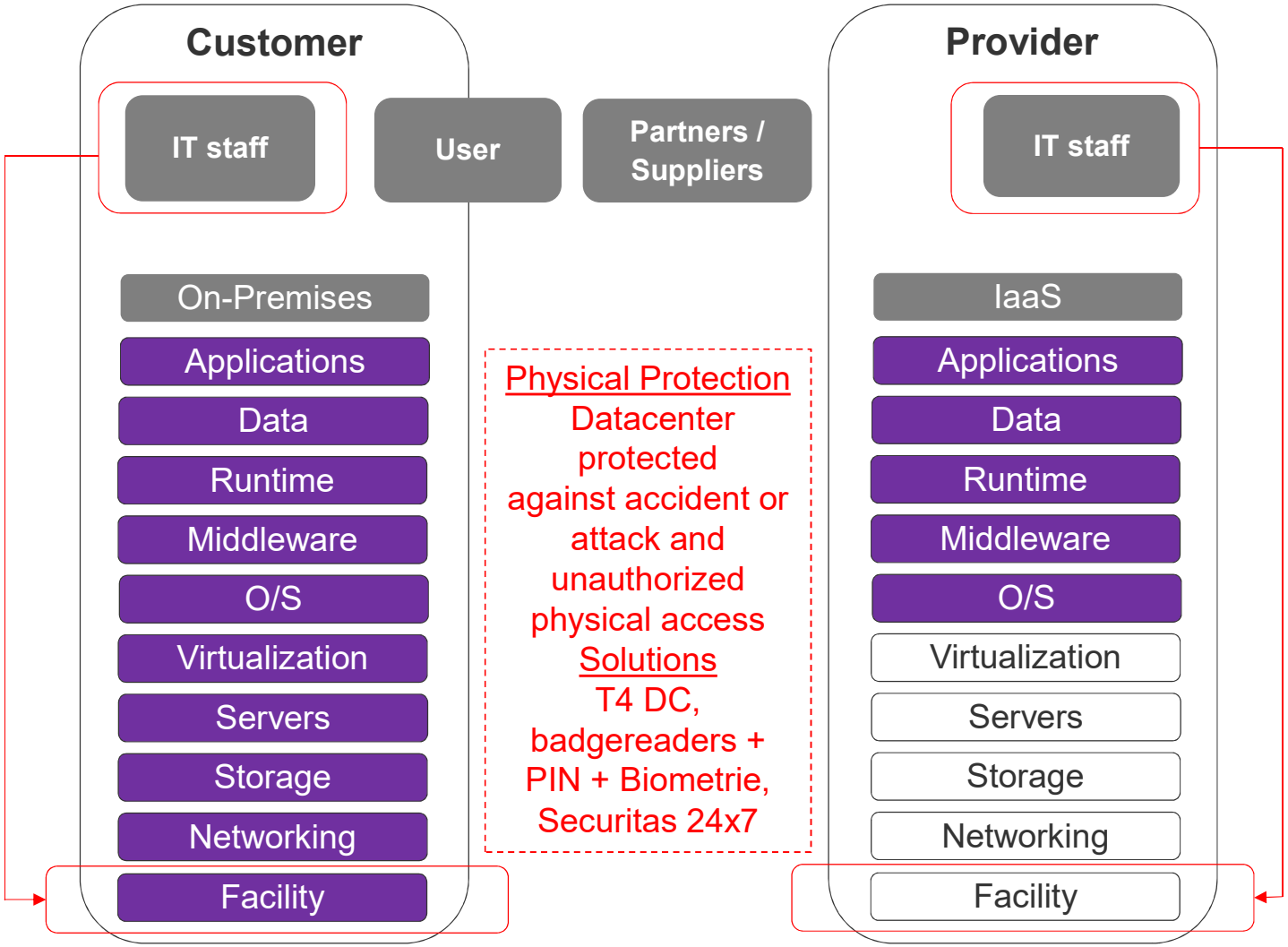
Eine vollständige und systematische Erfassung und Kategorisierung von Sicherheitsthemen ist aufwendig. Ein Ansatz könnten Security Architecture Domains sein, die Schutzmassnahmen beinhalten und Lösungsvarianten aufzeigen.

Security Architecture Domains
Secure Development
System Security
Data Security
Secure Communications
Identity and Access Management
Security Analytics
Security Processes



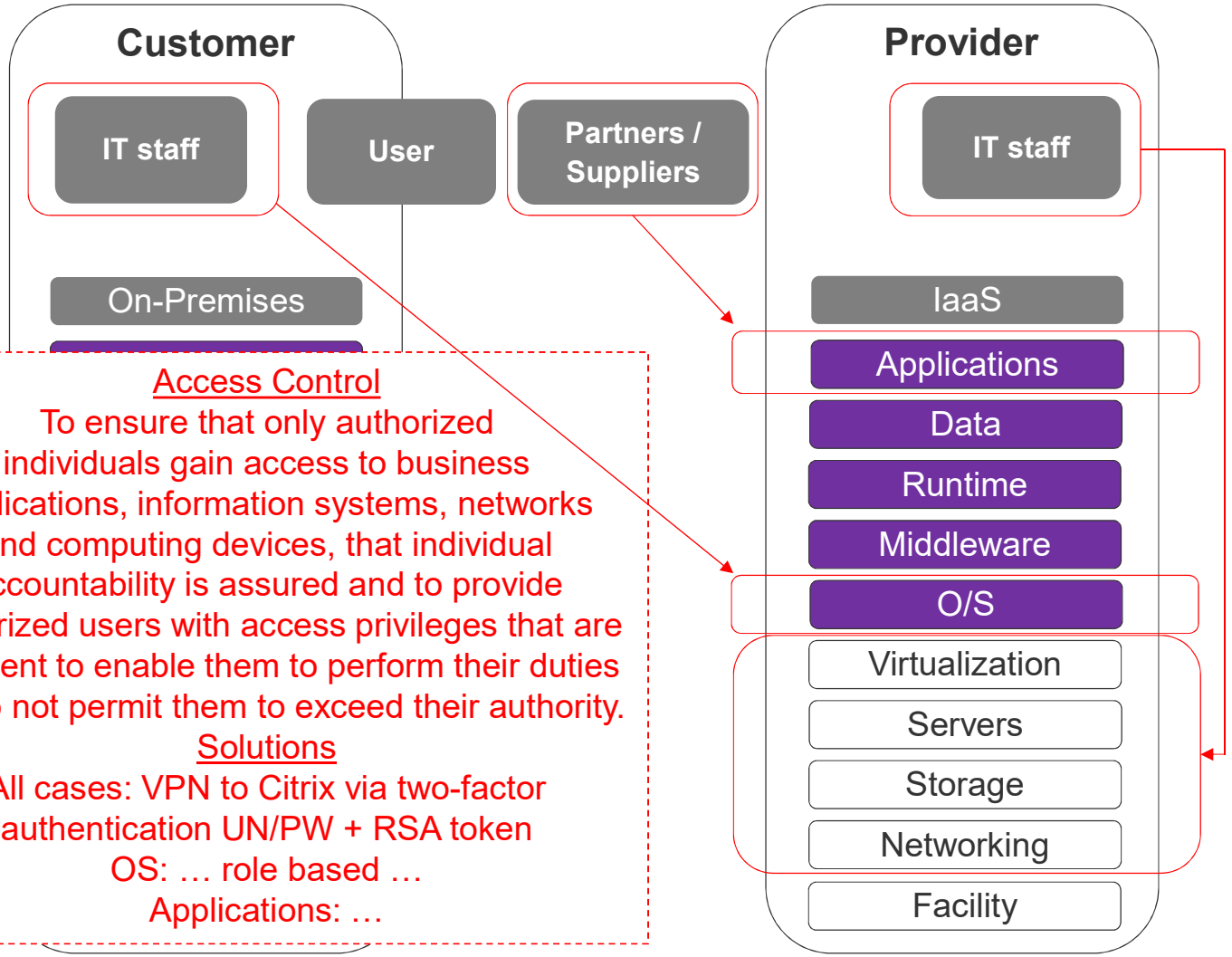
Herausforderungen: Security Architecture Domains – Beispiel 1

Security Architecture Domains
Secure Development
System Security
Data Security
Secure Communications
Identity and Access Management
Security Analytics
Security Processes



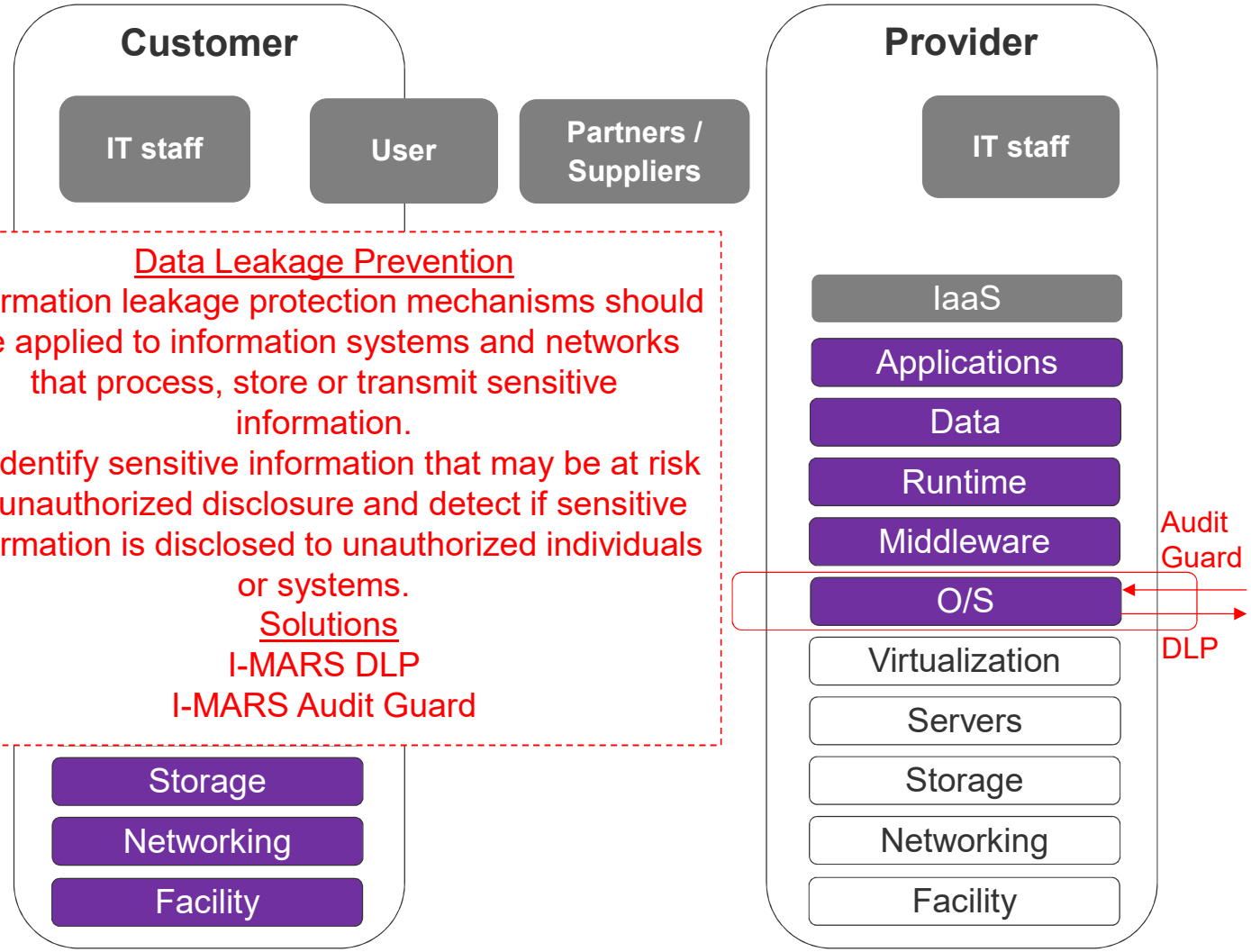
Herausforderungen: Security Architecture Domains – Beispiel 2

Security Architecture Domains
Secure Development
System Security
Data Security
Secure Communications
Identity and Access Management
Security Analytics
Security Processes



Herausforderungen: Security Architecture Domains – Beispiel 3

Security Architecture Domains
Secure Development
System Security
Data Security
Secure Communications
Identity and Access Management
Security Analytics
Security Processes



1. On-Premise to Cloud
2. Herausforderungen
3. Massnahmen
4. Fazit

Sourcing

Journey to Hybrid IT

Die grösste Hürde

Schutzziele, Compliance und Governance

Shared Responsibility Model

Security Architecture Domains

Internes Verständnis schaffen

Evaluation Cloud Provider

Massnahmen: internes Verständnis schaffen

Um ultimativ geeignete Provider zu evaluieren empfehlen wir folgende grobe interne Vorarbeiten:

- Transparenz über Security, Compliance- und Governancevorgaben in der sich befindenden Branche schaffen (dies umfasst insbesondere auch das Thema Datenklassifikation und daraus ableitenden Vorgaben zum Schutzbedarf)
- Klarheit über ICT Strategie schaffen (Hybrid IT Target Operating Model mit Weisungen zu make or buy, Migrationsverfahren, Entwicklungvorgaben nach Cloud native/DevOps und/oder konventionell)
- Mittels Shared Responsibility Model die Fertigungstiefen ausdetaillieren
  - was produziere ich für welchen Fall selber, was soll der Provider übernehmen?
  - konkreten Sicherheitsbedarf pro Fertigungstiefe festlegen
  - erste Vorselektion von potentiellen Providern
- Provider Evaluation durchführen (siehe folgende Slides)

Alternativ: Professional Service von Swisscom im Kontext der "Journey to the Cloud" anfordern ☺

Massnahmen: Evaluation Cloud Provider - nach CSCC

Für eine selbständige Evaluation eines potentiellen Cloud Providers verweisen wir auf das "Cloud Standards Customer Council CSCC" mit den 10 umfassenden Schritten zur Evaluation von Cloud Security. Die 10 Schritte lauten zusammengefasst wie folgt:

1. Ensure effective governance, risk and compliance processes exist
2. Audit operational and business processes
3. Manage people, roles and identities
4. Ensure proper protection of data and information
5. Enforce privacy policies
6. Assess the security provisions for cloud applications
7. Ensure cloud networks and connections are secure
8. Evaluate security controls on physical infrastructure and facilities
9. Manage security terms in the cloud service agreement
10. Understand the security requirements of the exit process

Der Provider sollte im Bereich von Compliance und Governance folgendes Minimum erfüllen:
Datenschutzgesetze
IT Grundschutz (BSI)
ISAE 3402
ISO 27001
Industriespezifika
Beachte: das Recht für ein eigens angeordnetes (ggf periodisches) Audit muss der Provider einräumen!

Quelle: https://www.omg.org/cloud/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

Massnahmen: Evaluation Cloud Provider – knackige Fragestellungen

- What are the access controls to your information when it's stored in the cloud? How do you monitor them? Who has access to the data, server rooms and the facilities?
- How will your cloud provider interact or participate during investigations, litigations, and legal holds?
- Do you have governance over and/or the "right to audit" your cloud provider's service, security, and access controls?
- What's the cloud provider's obligation to release data to third parties (law enforcement, government, previous employees)
- Who works for the provider? Are background checks performed? (Full time employees, contractors, vendors)
- Where will my data be stored, physically? In what countries/territories? Remember that physical server location might affect data privacy laws and regulations (e.g. US data stored on a server in EU country)

Quelle: https://slidex.tips/download/hidden-challenges-with-cloud-computing

1. On-Premise to Cloud

Sourcing

Journey to Hybrid IT

2. Herausforderungen

Die grösste Hürde

Schutzziele, Compliance und Governance

Shared Responsibility Model

Security Architecture Domains

3. Massnahmen

Internes Verständnis schaffen

Evaluation Cloud Provider

4. Fazit

Fazit

- **Cloud: the big vulnerability is the human factor**
- Vertrauen ist gut, Kontrolle ist besser: Aufgaben können an einen Provider delegiert werden, die Verantwortung aber nicht (z.B. DSGVO) !
- SLAs sind ein Schlüssel zum Erfolg (u.a. Response to incidents (data breach, regulatory inquiries and litigations), Data preservation, Physical locations for data storage, Right to audit)
- Klarheit zur Fertigungstiefe und des Schutzbedarfes schaffen, so wird die Erwartungshaltung an den Provider sowie auch an sich selber transparent – das erspart unnötige Überraschungen
- Einen potentiellen Provider sorgfältig evaluieren


Wem darf ich noch eine
Frage beantworten?

Quellen

https://www.forbes.com/sites/sungardas/2014/08/26/will-security-kill-the-cloud

https://www.infoworld.com/article/3201168/the-2-cloud-security-myths-that-must-die.html

https://www.gartner.com/en/newsroom/press-releases/2018-12-04-gartner-identifies-the-top-10-trends-impacting-infras

https://slidex.tips/download/hidden-challenges-with-cloud-computing

http://adeccogroup.ch/de/studien/fachkraeftemangel-index-schweiz/fachkraeftemangel-index-2018/

https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-says-cloud-computing-remains-top-emerging-business-risk

https://fr.slideshare.net/TanyaJanca/azure-cloud-security-workshop-115254662

https://www.rsaconference.com/writable/presentations/file_upload/spo3-t08-how_to_apply_a_zero-trust_model_to_cloud_data_and_identity.pdf

https://www.omg.org/cloud/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

Quelle: https://slidex.tips/download/hidden-challenges-with-cloud-computing