

Bezpečný cloud - ako na to....

pohľadom cloud poskytovateľa

—

Petr Leština
IBM Czech Republic



Agenda



Cloudová datová centra: certifikace & standardy (ISO, SOC, PCI, GDPR ...)

Služby IaaS a PaaS Cloud Computingu pohledem bezpečnosti

Zabezpečení dat: během přenosu / ukládání / archivace

Bezpečnostní monitoring a ověření kompatibility s bezpečnostními pravidly

Standardní smluvní dokumentace cloud poskytovatelů a ochrana dat

Nejčastější dotazy klientů spojených s ochranou dat v cloudu.



Důvěra a transparentnost

V IBM Cloudu vždy znáte fyzické umístění dat.

Pokud si klient explicitně nevyžádá nebo není předmětem servisní smlouvy -- IBM **nikdy** nepřistupuje k datům klienta – neprovádí manipulaci, zálohování, replikaci jak v rámci datacentra tak ani mezi zónami.

- ✓ Všechna klientská data jsou ve výhradním vlastnictví klienta včetně plné kontroly nad jejich správou.
- ✓ IBM nikdy nepoužije klientská data a bude s nimi manipulovat pouze na základě smluvní dokumentace.
- ✓ IBM nepoužije klientská data pro prodej nebo zprostředkování 3-tí straně.
- ✓ IBM Privacy guidelines jasně stanovují jaká data jsou použita pro jaký účel (fakturace apod.).



<http://www.ibm.com/cloud/data-security>

IBM Cloud Data Center Security

Fyzická a provozní bezpečnost je **základem** IBM Cloud infrastrukturní bezpečnosti. Veškerá datacentra jsou auditovaná na **SOC 2 Type II** a reporty jsou k dispozici klientům služby IBM Cloudu.

Data Centrum a Serverová místnost

- Data centers s plnou supervizí 24-hour security
- Server room nemá veřejný přístup „z ulice“
- Datacentrum obsluhované v režimu 24/7
- Vstup a výstupní dveře do datacenter jsou neoznačené
- Digital security video surveillance
- Biometric & Key Card pro přístupy (minimálně 2 faktorová autentizace)
- Server room se striktně limitovaným přístupem pouze pro zajištění provozu a kompatibility se standardy (audity apod.)
- Barcode-only identification on hardware; na žádném HW není jméno/logo klienta ani žádné další identifikující parametry



Provozní aspekty

- Engineers a technicians pravidelně trénováni na principy a procedury a auditováno 1x ročně
- Geographic redundancy pro všechny systémy pro zajištění kontinuity a vysoké dostupnosti
- Veškeré servery, HDD bezpečně smazány před uvolněním novému klientovi dle Department of Defense DoD 5220
- Certifikace SOC 1 + 2 Type II report

IBM Cloud Datacentra

- Standardizovaná Architektura
- x86, IBM POWER a System z Hardware
- Public, Private a Mgmt Network
- Management & Podpora
- SLA 99.9% a 99.99% pro cloud services



Single & Multi-zone regiony

Dallas | D.C. | Frankfurt | Tokyo | London | Sydney

Plánováno: Sao Paulo

+190 services

Public nebo private modely

60 Data Center

in 19 Countries

1st GDPR Compliant

Data Hyper protection and GDPR compliance

One Cloud Architecture

IoT, Watson, Data, IBM Z, Blockchain



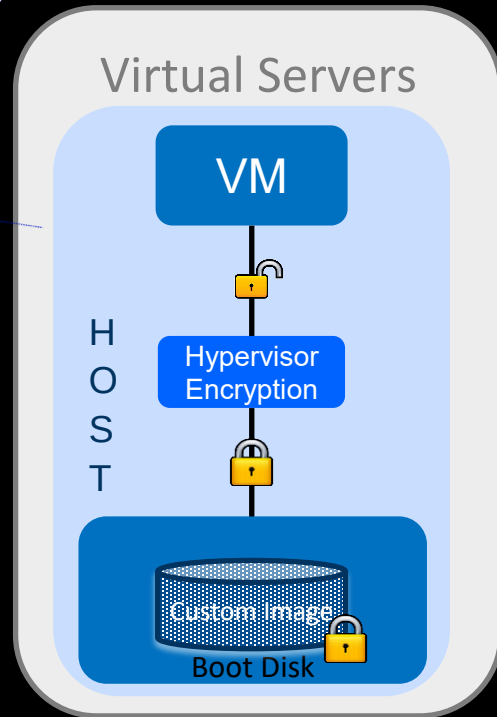
Šifrování a zabezpečení dat

Během přenosu (Data-In-Transit)

- HTTPS, SSL, a TLS při přenosu po internetu
- VPC/VPN gateway zajistí IPsec site-to-site link
- IBM Direct Link pro privátní linku
- Security Gateway
 - Juniper vSRX
 - ATT Virtual Router Appliance

Ukládání (Data-At-Rest)

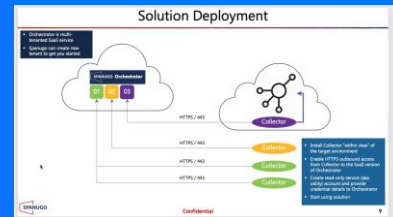
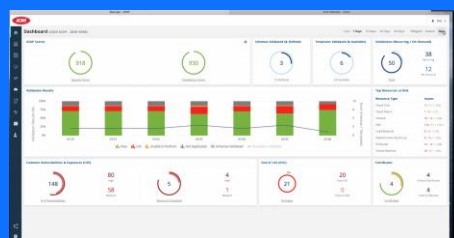
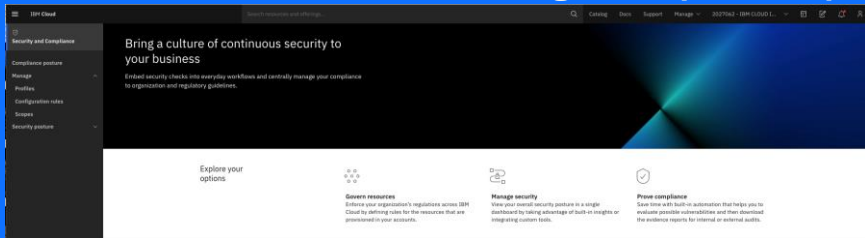
- Klient určuje mechanismus šifrování, s technologiemi Hytrust a BYOK/KYOK
- OS image šifrovaná BYOK/KYOK
- IBM Cloud hardware security modules (HSMs)
- File/Block Storage šifrovaná standardně AES-256
- Výpočetní výkon zabezpečený pomocí Intel TPM/TXT



Bezpečnostní monitoring v Cloudu

IBM Cloud Security and Compliance Center

Integrované prostředí pro správu a bezpečnostní monitoring



Bezpečnostní pravidla a principy

Bezpečnostní principy založené na NIST based control assessments.

[illegible]

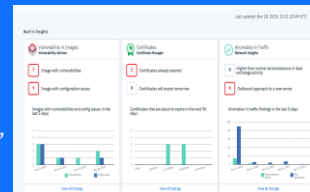
Řízení bezpečnostních konfigurací

Správa a řízení bezpečnostních parametrů pro IBM Cloud public services



Bezpečnostní náhled

Visualizace a
náhled na
zranitelnosti
network &
activity behavior,
expirace
certifikátů



IBM Cloud certifikáty

<https://www.ibm.com/cloud/compliance>

IBM Cloud a základní standardy

IBM Cloud Security Policy



Based on ISO27001

NIST SP800-53

Průmyslové a regionální certifikáty



SOC1, SOC2, SOC3



Germany



DoD DISA IL-2



ENS High Spain



FedRAMP**
High



Hébergeurs de Données de Santé (HDS)
Health Data Hosting



MTCS L3



Australia



ISO/IEC 9001



ISO/IEC 27001



ISO/IEC 27017



ISO/IEC 27018



ISO/IEC 22301



ISO 31000 Risk-Management



PCI DSS Level 1

Průmyslové a odvětvové certifikáty pro banky, telco, zdravotnictví a další segmenty



Germany – Federal Financial Supervisory Authority



STAR Level 1



Self Assessment



FISMA

Federal Information Security Modernization Act



GDPR



My Number Act Japan



EU-US

Aktuální certifikáty jsou on-line na webu a lze je zdarma downloadovat

Standardní smluvní dokumentace

Poskytuje klientovi jasně definované parametry cloud služeb včetně SLA, odpovědnosti, smluvních pokut a zpracování dat

Cloud Service Agreement

Všeobecné podmínky pro cloud služby

Service Description

Popis cloud služby (SLA, přístupy, podpora apod.)

Data Protection Addendum

Zabezpečení dat a ochrana soukromí

Security & Privacy Principles

Obecné bezpečnostní principy

Nejčastější dotazy od klientů...



Otázka #1: *„Kde jsou moje data? Mohu znát fyzickou adresu datacentra cloudového poskytovatele? Lze je auditovat?“*

Otázka #2: *„Jak je to se šifrováním dat na sdíleném úložišti typu Block/NFS File Storage? Co se stane s poškozenými disky a jak jsou likvidovány?“*

Otázka #3: *„Jak je to s EXIT strategií? Mohu si data z cloudu kdykoli odnést/exportovat a provoz kdykoli ukončit?“*

