A FELHŐALAPÚ RENDSZEREK BIZTONSÁGI KOCKÁZATAI ÉS MEGFELELÉSI KÉRDÉSEI

Farkas Imre CISSP CISA CRISC CGEIT CCSK
Cégvezető, FORTIX Consulting Kft.

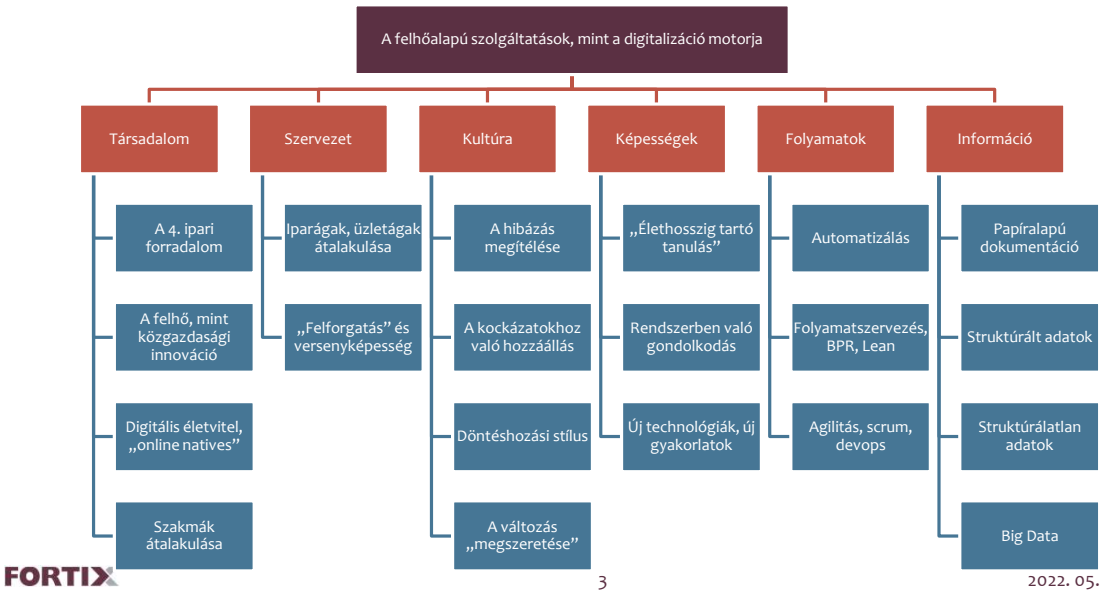
1

MIRŐL LESZ SZÓ?

- Felhő: Lehetőségek és Kockázatok
- Milyen irányban indultunk?
- Információvagyon a felhőben; avagy:
  Hol van a felhőben a védendő érték?
- Felhő = nagyobb biztonság, ha jól csináljuk!
- Kontroll-bevezetés és –validáció
- Bizonyosságszerzés és tanúsítás
- Hogyan fogjunk hozzá (biztonságosan)?

2

A DIGITALIZÁCIÓ CSAK TECHNOLÓGIAI KÉRDÉS?



3

A „FELHŐ” LEHETSÉGES ELŐNYEI / 1: *STABILABB ÜZLETI MŰKÖDÉS ÉS KOCKÁZATCSÖKKENTÉS*

4

A „FELHŐ” LEHETSÉGES ELŐNYEI / 2:
A SZERVEZETI FEJLŐDÉS KATALIZÁLÁSA

5

A FELHŐ KOCKÁZATAI / 1:
„KLASSZIKUS” KOCKÁZATOK ÉS MEGFONTOLÁSOK

- **Jogszabályi, hatósági és szabályzati megfelelés**
- **Fizikai biztonság**
- BC/DR tervezés, redundanciák és **tesztelés**
- **SLA-k**
- **Breakglass**
- DDoS

6

A FELHŐ KOCKÁZATAI / 2:
HANGSÚLYOSABBÁ VÁLÓ KOCKÁZATOK

How confident are you that your IT department knows about all cloud storage providers being used to store corporate data?

- Csökkenő transzparencia
- Összebútorozás
- Megoszló „felelősségek”
- ← Shadow IT / Everything-as-a-Service
- Lokáció
- Egyoldalú változtatások
- „Lock-in”
- Az ellátási **lánc**
- A Management plane
- Economic DoS
- Authentikáció, titkosítás sérülése

FORTIX Grafika forrás: Helpnetsecurity 7 2022. 05. 11.

7

INFORMÁCIÓVAGYON A FELHŐBEN; AVAGY:
HOL VAN A FELHŐBEN A VÉDENDŐ ÉRTÉK?

Számítási erőforrások (compute)	Tárolás (storage)	Hálózat (network)
• Hipervizorok, virtuális gépek • Konténerkezelők, konténer instance-ok • Platformok, „serverless” • **API-k!!**	• Kötetek • Objektumtárak • Konténerképek (images) • Adatbázisok • Konfigurációs adatok (infrastructure as code) • Titkok (secrets): tanúsítványok, kulcsok • Forráskód!!	• Virtuális hálózat • Tartalomkiszolgáló nálózat (CDN) • DNS bejegyzések • Útválasztási konfiguráció (pl. BGP) • SSL/TLS tanúsítványok • Terheléselosztók, proxyk, alkalmazástűzfalak

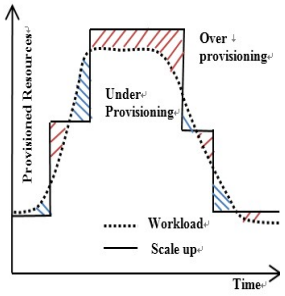
Forrás: Dotson: Practical Cloud Security

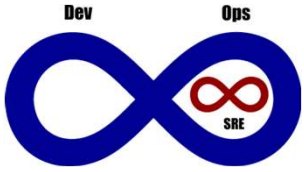
FORTIX 8 2022. 05. 11.

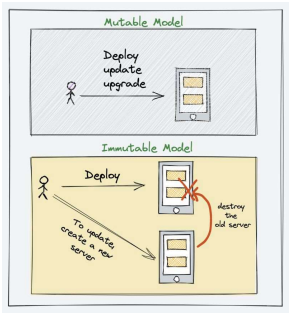
8

FELHŐ = NAGYOBB BIZTONSÁG, HA JÓL CSINÁLJUK!

Architektúra | **Autoscaling** | **Automatizáció** | **Immutable**



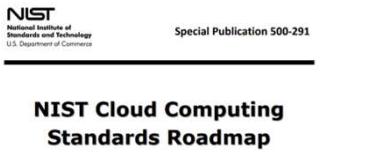


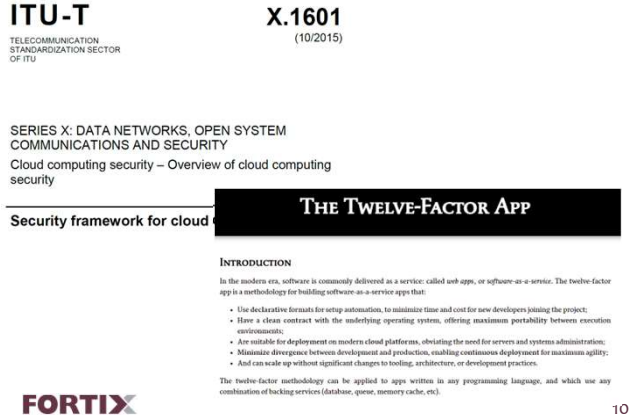


Forrás: Medium | Forrás: Researchgate | Forrás: Jonathan Hall | Forrás: Devopslearners

9

KONTROLL BEVEZETÉS ÉS VALIDÁCIÓ





10

BIZONYOSSÁGSZERZÉS ÉS TANÚSÍTÁS

INTERNATIONAL STANDARD ISO/IEC 27017

First edition 2015-12-15

Information technology — Security techniques — Code of practice for ed on

Cloud Controls Matrix (CCM)

- A&A Audit and Assurance
- AIS Application & Interface Security
- BCR Business Continuity Mgmt & Op Resilience
- CCC Change Control and Configuration Management
- CEK Cryptography, Encryption and Key Management
- DCS Datacenter Security
- DSP Data Security and Privacy
- GRC Governance, Risk Management and Compliance
- HRS Human Resources Security

INTERNATIONAL STANDARD ISO/IEC 27018

Second edition 2019-01

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

EU Cloud Code of Conduct

EU CLOUD COC

DORA Digital Operational Resilience Act

AICPA Service Organization Control Reports — AICPA SERVICE ORGANIZATIONS — SOC aicpa.org/soc — Formerly SAS 70 Reports

A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről

I. Az ajánlás célja és hatálya

Jelen ajánlás célja, hogy a pénzügyi közvetítőrendszer szereplői számára gyakorlati útmutatást adjon a közösségi és publikus felhőszolgáltatások igénybevételéből eredő kockázatok kezeléséhez, valamint a vonatkozó nemzeti és európai uniós jogszabályokban, egyéb szabályozó eszközökben foglalt rendelkezések[1] egységes alkalmazásához. Ennek érdekében az ajánlás – a felhőszolgáltatás életciklusát és az alapelveket követve – meghatározza a szerződések elvárt minimumkövetelményeit, ismerteti a kezelendő kockázatokat, az elvárt kontrollintézkedéseket és a pénzügyi közvetítőrendszer felügyeletével kapcsolatos feladatkörében eljáró Magyar Nemzeti Bank (a továbbiakban: MNB) jelen ajánlás tárgykörét érintő ellenőrzéseinek fő szempontjait.

Federal Office for Information Security

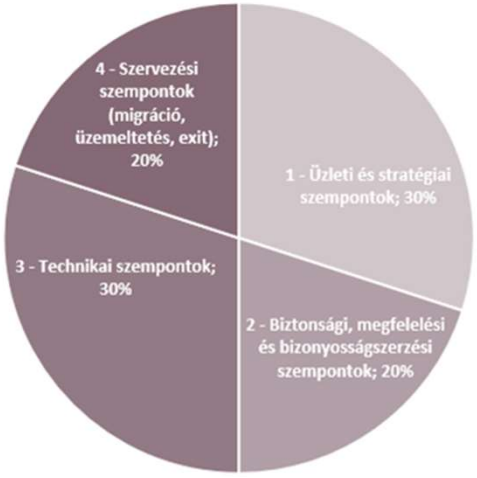
Cloud Computing Compliance Criteria Catalogue (C5)

FORTIX

11

HOGYAN FOGJUNK HOZZÁ A „FELHŐSÍTÉSNEK”?

1. Értékeljük, mink van, és mik a céljaink!



2. Építsünk stratégiát és induljunk el! **(6R)**

- Megtartás (**retain**)
- Kiváltás (**replace/repurchase**)
- Átemelés (**rehosting**)
- Platformváltás (**replatforming**)
- Újrafejlesztés (**refactoring/re-architecting**)
- Kivezetés (**retire**)

FORTIX

12

EGY PRAKTIKUS ÁTTEKINTÉS A FELHŐBIZTONSÁGRÓL...

TOVÁBBI REFERENCIÁK

- A Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlása az informatikai rendszer védelméről
- A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről (Felhőajánlás)
- A Magyar Nemzeti Bank Gyakori kérdések és válaszok felhőszolgáltatások igénybevételével kapcsolatban (GYIK) dokumentuma
- ENISA Cloud Computing Benefits, risks and recommendations for information security
- ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements
- CSA Cloud Controls Matrix (CCM) v4
- EU Cloud Code of Conduct
- ITU-T X.1601 Security framework for cloud computing
- MITRE ATT@CK
- NIST SP 800-145

KÉRDÉSEK?

MAGABIZTONSÁGOT ADUNK!

Köszönöm a megtisztelő figyelmet!

Farkas Imre