





A FELHŐALAPÚ RENDSZEREK BIZTONSÁGI KOCKÁZATAI ÉS MEGFELELÉSI KÉRDÉSEI

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







1

2022. 05. 11.


1




MIRŐL LESZ SZÓ?



- Felhő: Lehetőségek és Kockázatok
- Milyen irányban indulunk?
- 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)?

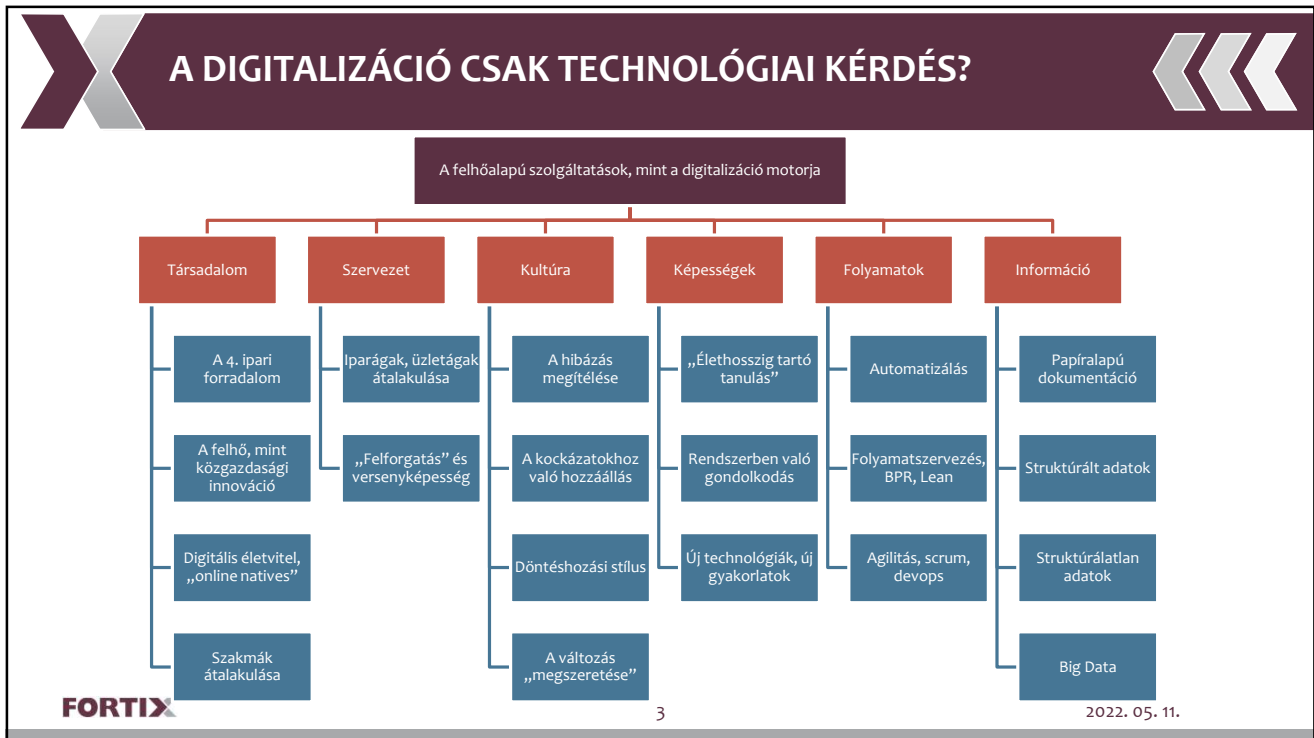




2

2022. 05. 11.

2



3



4

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

Gyors piaci innováció

Újraalapozás lehetősége

Folyamat-optimalizálás

Új szervezeti és egyéni képességek kialakítása

Finanszírozás átalakítása

A felsővezetői kör figyelme

FORTIX

5

2022. 05. 11.

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

**BUSINESS
as USUAL**

FORTIX

6

2022. 05. 11.

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 „felelőségek”
- ← 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)

- Hipervizorok, virtuális gépek
- Konténerkezelők, konténer instance-ok
- Platformok, „serverless”
- **API-k!!**

Tárolás (storage)

- Kötetek
- Objektumtárak
- Konténerképek (images)
- Adatbázisok
- Konfigurációs adatok (infrastructure as code)
- Titkok (secrets): tanúsítványok, kulcsok
- Forráskód!!

Hálózat (network)

- Virtuális hálózat
- Tartalomkiszolgáló hálózat (CDN)
- DNS bejegyzések
- Útválasztási konfiguráció (pl. BGP)
- SSL/TLS tanúsítványok
- Terheléselosztók, proxy, alkalmazástűzfalak

FORTIX

8

Forrás: Dotson: Practical Cloud Security

2022. 05. 11.

8

X FELHŐ = NAGYOBB BIZTONSÁG, HA JÓL CSINÁLJUK!

Architektúra

Autoscaling

Automatizáció

Immutable

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

9
2022. 05. 11.

9

X KONTROLL BEVEZETÉS ÉS VALIDÁCIÓ

With our global community of cybersecurity experts, we've developed CIS Benchmarks: more than 100 configuration guidelines across 25+ vendor product families to safeguard systems against today's evolving cyber threats.

join a Community

IS AUDIT/ASSURANCE PROGRAM

Cloud Computing

Special Publication 500-291

ITU-T X.1601
(10/2015)

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cloud computing security – Overview of cloud computing security

Security framework for cloud

THE TWELVE-FACTOR APP

INTRODUCTION

In the modern era, software is commonly delivered as a service: called web apps, or software-as-a-service. The twelve-factor app is a methodology for building software-as-a-service apps that:

- Use declarative formats for setup automation, to minimize time and cost for new developers joining the project;
- Have a clear contract with the underlying operating system, offering maximum portability between execution environments;
- Are suitable for deployment on modern cloud platforms, obviating the need for servers and systems administration;
- Minimize divergence between development and production, enabling continuous deployment for maximum agility;
- And can scale up without significant changes to tooling, architecture, or development practices.

The twelve-factor methodology can be applied to apps written in any programming language, and which use any combination of backing services (database, queue, memory cache, etc).

Top 10 Cloud Providers

10
2022. 05. 11.

10

BIZONYOSSÁGSZERZÉS ÉS TANÚSÍTÁS

INTERNATIONAL STANDARD ISO/IEC 27017
FIRST EDITION 2015-12-15

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

DORA Digital Operational Resilience Act

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

I. Az ajánlás célja és hatálya

Jelen ajánlás célja, hogy a pénzügyi közvetítőrendszer szereplői számára gyakorlati útmutatást adjon a közbizségi és publikus felhőszolgáltatások igénybevételéből eredő kockázatok kezeléséhez, valamint a vonatkozó nemzeti és európai uniós jogszabályokban, egyéb szabályozó eszközökben foglalt rendelkezések¹ egyrészleges alkalmazásához. Ennek érdekében az ajánlás – a felhőszolgáltatás életciklusát és az alapelvetek kivételét – meghatározza a szerződések kívánt minimumkövetelményeit, ismerteti a kezelendő kockázatokot, az elvárt kontrollintézkedéseket és a pénzügyi közvetítőrendszer felügyeletével kapcsolatos feladatkörében eljáró Magyar Nemzeti Bank (a továbbiakban: MNB) jelen ajánlás tárgyát érintő ellenőrzéseinek fő szempontjait.

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

Submissions: CAIS, Certification

Cloud Controls Matrix (CCM)

- AAA Audit and Assurance
- AIS Application & Interface Security
- BCK 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

FORTIX

EU Cloud Code of Conduct

AICPA Service Organization Control Reports (SOC)

Formerly SAS 70 Reports

Federal Office for Information Security

Cloud Computing Compliance Criteria Catalogue (C5)

2022. 05. 11.

HOGYAN FOGJUNK HOZZÁ A „FELHŐSÍTÉSNEK”?

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

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

2022. 05. 11.

EGY PRAKTIKUS ÁTTEKINTÉS A FELHŐBIZTONSÁGRÓL...



FORTIX

2022. 05. 11.

13

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

FORTIX

14

2022. 05. 11.

14

KÉRDÉSEK?

MAGABIZTONSÁGOT ADUNK!



Köszönöm a megtisztelő figyelmet!

Farkas Imre

FORTIX

15

2022. 05. 11.