HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI
SZAKOSZTÁLY

Elektronikus Információs Rendszerek (EIR) biztonsága – hasonlóságok és különbségek a földön és a publikus felhőben.

Hétpecsét Konferencia 2023. március 22.

Oláh István – EIVOK alelnök, Óbudai Egyetem BDI.
HTE Információbiztonsági Szakosztály – EIVOK
istvan.olah@hte.hu; olah.istvan.op@gmail.com;

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Témakörök

Forrás: bitport.hu

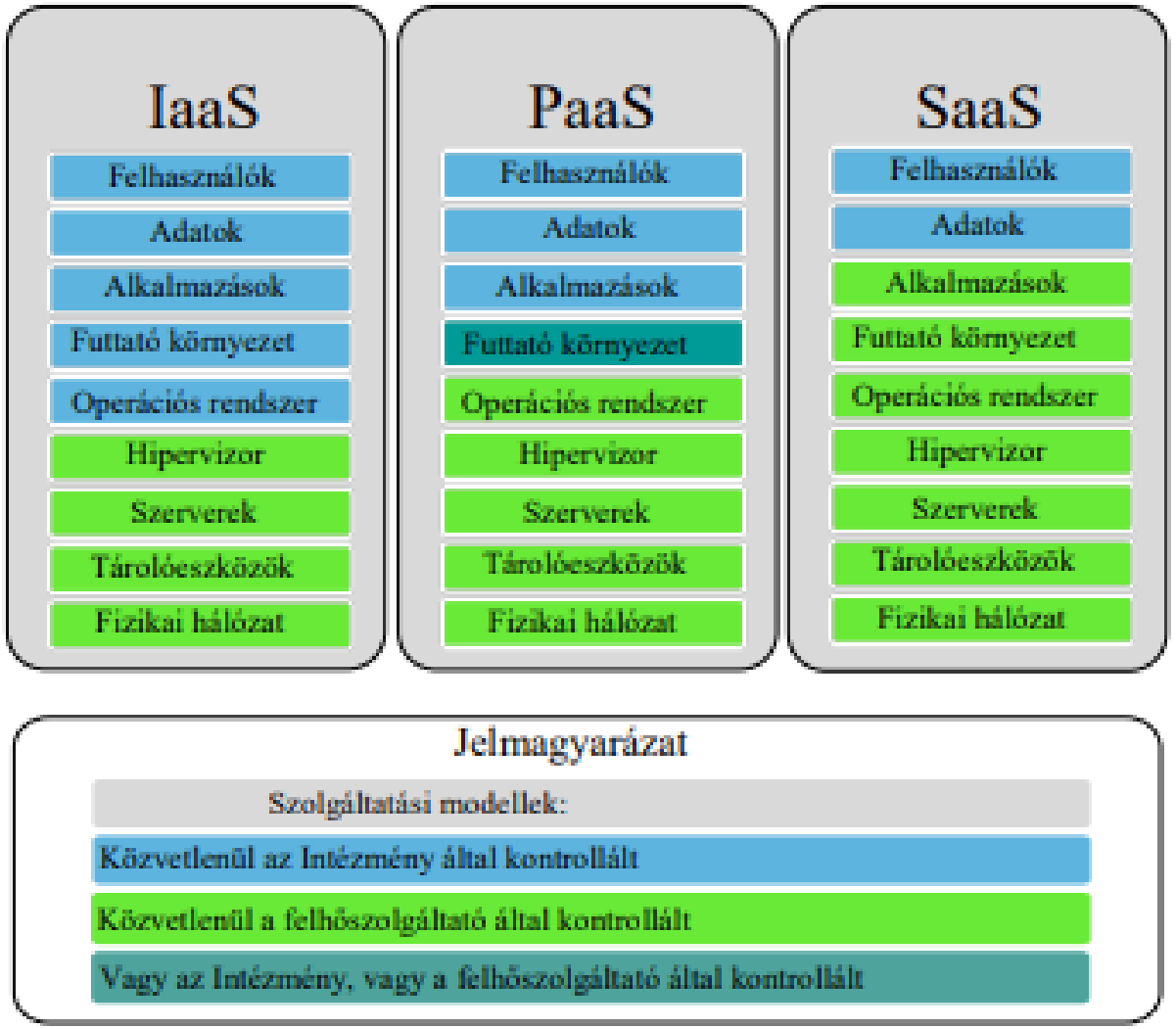
- Milyen „felhős” esetek, szolgáltatások léteznek.
- Szabad-e, és mire használni a Felhőt.
- A Felhő és a B,S,R.
- Tervezés, HLD, LLD, BRD.
- BCP, DRP, egy felhővel.
- Adatink egy publikus felhőben.
- SLA-k.
- *„Elnyomási”* hatások.
- Egy felhő auditja.
- Szolgáltatási láncok.
- Egyéb *„kiskérdések”*.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

A felhő fogalma, és felelősségi kérdései?

- **Az adat és felhasználók mindig az intézmény kontrollja alatt állnak!**
- Ezt hogyan lehet elérni? Titkosítással!
- A titkosításon túl a kulcsok kezelési folyamatát is külön szükséges átgondolni.
- IV.1.2. A tárolt adatok biztonsága:

*„e) a kockázatelemzés alapján kritikus funkcionalitás vagy rendszer esetén **az Intézmény gondoskodik az adatmentések felhőszolgáltatótól független tárolásáról is**; a függetlenül tárolt mentések rendszerességét a kockázatok és jogszabályi elvárások figyelembevételével határozza meg.”*



Forrás:
https://www.mnb.hu/letoltes/4-2019-felho.pdf

XaaS ?

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

+ Address Verification as a Service
+ **Anything as a Service**
+ API as a service (APIaaS) Application
+ Delivery as a Service
+ Application Platform as a Service
+ Architecture as a Service
+ Authentication as a Service
+ Backend as a Service
+ Backup as a Service
+ Big Data as a Service
+ Broker as a Service
+ Business as a Service
+ Business Process as a Service
+ Cloud Load Balancers as a Service
+ Cloud Search as a Service
+ Collaboration-as-a-Service
+ Commerce as a Service
+ Communication as a Service
+ Computing as a Service
+ Contact Center as a Service
+ Conversations as a Service
+ Data as a service
+ Database as a service
+ Desktop as a Service
+ Development as a Service
+ DevTest as a Service
+ Disaster Recovery as a Service
+ Drupal as a Service
+ Email as a Service
+ Encryption as a Service
+ Enterprise Resource Management as a Service
+ Ethernet as a Service
+ **Everything as a Service**
+ Firewall as a Service
+ Framework as a Service
+ Globalization as a Service
+ Hadoop as a Service
+ Hardware as a Service
+ High Performance Computing as a Service
+ Identity as a Service
+ (Infrastructure PaaS)
+ Insight as a Service
+ Integrated Development Environment as a Service
+ Integration as a Service Integration Platform as a Service
+ Integration Platform as a Service
+ **IT as a Service**
+ Java Platform as a Service
+ Knowledge as a Service
+ Light as a Service
+ Logon as a Service Management as a Service
+ Mashups as a Service
+ Message Queuing as a Service
+ Metal as a Service
+ Mobility as a Service
+ Mobility Backend as a Service
+ Monitoring as a Service
+ Network Access Control as a Service
+ Network as a Service
+ Operations as a Service
+ Optimization as a Service
+ Payment as a Service
+ Quality as a Service
+ Query as a Service
+ Recovery as a Service
+ Remote Backup as a Service
+ Risk Assessment as a Service
+ Robot as a Service
+ Security as a service
+ Service Desk as a Service
+ Solutions as a Service
+ Storage as a Service
+ Telepresence as a Service
+ Test environment as a Service
+ Testing as a Service
+ Transport as a Service
+ Unified Communications as a Service
+ User Interface as a Service
+ Video Conferencing as a Service
+ Video Surveillance as a Service
+ Voice as a Service
+ Website as a Service

+ **Mélytanulás**
+ **Kvantumszámítástechnika**

Forrás: Koczka Ferenc, okosóra előadása az OTP Bank Nyrt-ben

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

As a Service ?

- PhaaS Phishing as a service.
  - PhpaaS Phishing protection as a service.
- VaaS virus as a service.
  - VPaaS virus protection as a service.
- MaaS malware as a service.
  - MPaaS malware protection as a service.
- SaaS spam as a service.
  - SFaaS spam filter as a service.
- ..
- Any hacking as a service.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Lehet e felhőt használni, és mire?

- **Mindent is lehet! jogszabályi megkötés nincs az Ibtv-n kívűl**, de:
  - Tervezési lépések elején érdemes átgondolni a kivonási stratégiát is, amely fontosabb mint elsőre gondolnánk.
  - Szükséges a felhőben lévő IT platform konfiguráció mentésére, de hol legyen a mentett állomány?
  - A BCP, DRP folyamatok átgondolása, milyen „VAS”-ra lehet menni, ha nincs saját infrastuktúra?
  - Multi-Cloud? Hibrid-Cloud? A rendszereink tudnak-e így működni, és a gazdasági modell ekkor mit mutat?
  - ADATKÖRÖNKÉNT végzett kockázatelemzés tud segíteni abban, hogy mit szabad és mit nem a felhőben tárolni, vagy kizárólag egy felhőszolgáltatónál tárolni.
  - A BSR elemek közül eddig B és az S kerül elő részben a titkosítási eljárások vetületében.
  - Lehetőség szerint ne a szolgálató eszközein képezzük a kulcsokat, mert a maradványinformációkra is gondolni érdemes.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

A Felhő „ R” I.

- Nincs egyetlen felhő szolgáltató amely képes lenne a 100% SLA-ra, az adott cég termékével kapcsolatos problémákról sok szakmai cikk jelent meg főleg a levelezéssel összefüggő napi problémákról.
- Nincs 100%-s internetkapcsolat sem, nagyon sok ok miatt.
- A távolságnak + a BSR elemeknek (pl: a titkosítás is időbe kerül, időben „ára” van, azaz ha van olyan folyamat az IT-üzemben, amelyhez szükségesek a mentett adatok is, akkor egy HLD, LLD tervezést szükséges végezni a folyamatok IT vetületeire, mert a késleltetéseket (latency) modellezni kell.
- A felhő és szükséges Internet kapcsolat, ez jelentősen megnövelheti kitettségi kockázatot, amely a felhasználói élményre gyakorolt hatáson túl gondot okozhat az összetett folyamatokban, mert időtúllépés (time out) miatt hibára mehetnek a folyamatok stochasztikusan.
- Szükség lehet Qos képes hálózati eszközökre, amelyeket esetenként be kell szerezni.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

A Felhő „ R” II.

- Szükség lehet Qos képes hálózati eszközökre, amelyeket esetenként be kell szerezni.
- Fentiek miatt a felhőszolgáltatóval kötendő szerződésekbe javasolt egy referencia mérést is rögzíteni, amely alapján a teljes jelfolyam különböző pontjain az idők mérhetők.
- „Képernyőtől az adatig” oda és vissza tervezési szemlélet fontossága.
- Az „*Elnyomási Hatás*” az Internet és a TELKÓ szolgáltatók csak X szakaszra adnak bármilyen műszaki garanciákat, de a felhős „infra” ezen túl van…
  - A magas rendelkezésre álláshoz nemzetközi bérelt adatkapcsolatra is szükség lehet!
  - A felhőszolgálató is *„érdekesen….”* skálázza az erőforrásait!

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

A Felhő „ R”, „B”

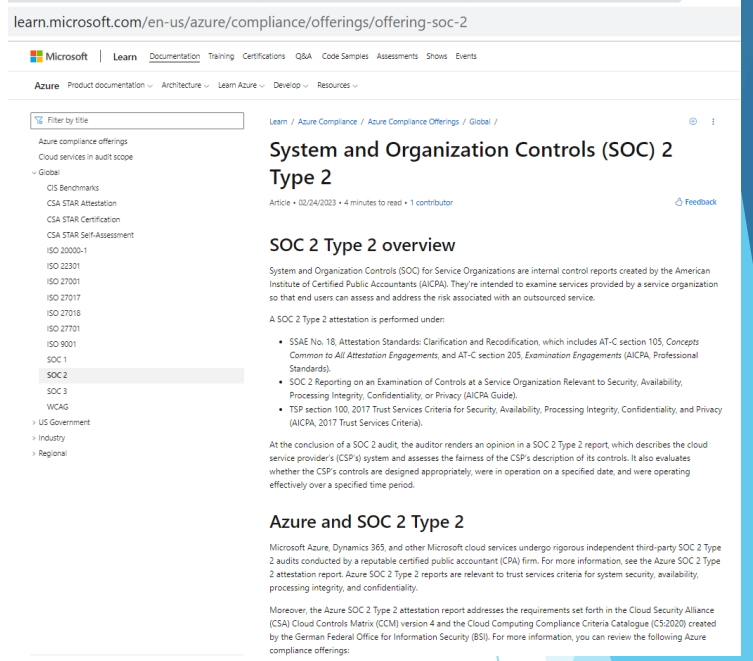
- A felhő IT üzemből származó adatokat érdemes a saját menedzsment rendszerben folyamatosan feldolgozni előjelző és hiba szintek meghatározásával.
- A SIEM hogy? Használjuk-e szolgáltató megoldását?
  - Lehetőleg ne csak azt, mert Ki Őrzi, az Őrzőket ekkor?
  - Ha igen , akkor is a logok releváns részét máshol menteni és feldolgozni javasolt!
- A szerződésekben az általános rendelkezésre álláson túl a szolgáltató be és kilépési pontja közti elvárt időt mint SLA elemet szükséges jogilag kezelni.
- A gazdasági számításokba a nem elérhetőség hatásait nem szokták figyelembe venni, ezért a többi rendszer esetében ezt is javaslom számolni, figyelembe venni, mint a jelenben nem létező, de a felhő által okozott többletráfordítások nem EIR vetületeit.
- Ez nagyon sok féle lehet de egy egyszerű példa, ha a felhő miatt átlagosan 2 nappal később mennek ki a számlák (ez tapasztalti tény), akkor a cash finanszírozás X forinttal kerül többe (itt az elmaradt napi kamat is számít), és sok sok példa lehetne még…..

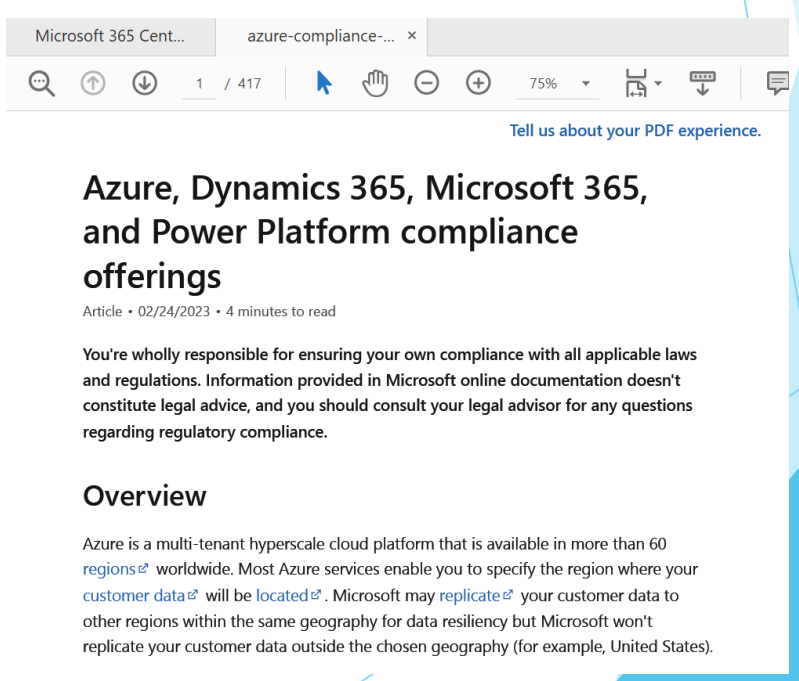
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

A Felhő auditja I.

- Felhőszolgáltató igénybe vételével kapcsolatos beszerzéskor EIV-ként érdemes elkérni a szolgáltatást vizsgáló auditok dokumentációját.

- Akinek van, jellemzően a tanúsítványt publikálja az Interneten, de abból valójában semmit nem lehet megtudni, mert az értelmezésükhöz be kell szerezni a vizsgálati profilt, módszertant és az audit tervet is. Ezekből lehet látni a mit és milyen szinten tud nyújtani a szolgáltató ami általában nem az a szint amit hirdet magáról!





Forrás:https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-soc-2

A Felhő auditja II.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

- Felhőszolgáltató dokumentumai elérhetőek.
- Több ezer oldal 10% url.
- A dokumentumok dinamikusak, részei a szerződésnek!


Microsoft

Microsoft Cloud Mapping
for Financial Institutions in Europe

Version: February 2023

1

Microsoft

EBA, EIOPA and ESMA guidelines that we have not included in the mapping below as these fall entirely within the responsibility scope of financial institutions' arrangements internally and are not specifically related to outsourcing.

4. While Microsoft provides a range of tools and information for customers and potential customers in its Compliance Documentation, on its Service Trust Portal and Trust Center to support firms through their regulatory due diligence and risk assessments, this mapping is a further tool intended to assist financial institutions interested in using Microsoft Online Services.

MAPPING

Item	Reference	Requirement	Microsoft commentary / How and where is this dealt with in the Microsoft Agreement?	Microsoft Agreement reference
		General		
1.	EBA 74 EIOPA 36 ESMA 26	**Rights and obligations** to be clearly allocated in a written agreement. The agreement for critical or important functions must set out:	The rights and obligations of the parties are set out in the Microsoft Agreement.	N/A
2.	EBA 75(a) EIOPA 37(a) ESMA 28(a)	**Services:** A clear description of the outsourced cloud services and type of support services;	The Online Services are described in the Microsoft Agreement. An online description is also available here: • Microsoft 365 Service Description • Dynamics 365 Service Description • Directory of Azure Cloud Services The support services, including Professional Services, are described in the DPA and in the Master Business Services Agreement. The Microsoft Cloud for Financial Services documentation provides capabilities to manage financial services data at scale and makes it easier for financial services organizations to deliver differentiated experiences, empower employees, and combat financial crime. It also facilitates security, compliance, and interoperability.	N/A
3.	EBA 75(b) EIOPA 37(b) ESMA 28(b)	**Term:** Start and end date and notice periods;	Refer to the Microsoft Agreement. In general, standard EA Enrollments have a three-year term and may be renewed for a further three-year term.	N/A

Version: February 2023

3

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

A Felhő szolgáltatási láncok

- Egy felhőszolgáltatóval szerződünk, de pl. egy SaaS esetében több szolgáltató érintett:
  - Szolgáltató.
  - Szolgáltatás.
  - Adatközpontok.
  - Szolgáltatás szintje XaaS.
  - Szerződéses kapcsolat direkt, indirekt.
  - Joghatóság.
  - A szerződések eljárási joga!

+ „Fül” az „OVI” táblában és minden lehetséges esetre az az összes kontrollt.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

A Felhő egyéb kérdései

- A felhőszolgáltató szerepe GDPR szerint, mert jellemzően adatfeldolgozónak számít.
- A felhőszolgáltató kiszervezett tevékenység szerepe, mert jellemzően annak számít.
- A felhőszolgáltató **szavatoló tőke helyzete**, azaz a nem működésből fakadó lehetséges közvetlen és közvetett károkat mekkora mértékben képes megtéríteni, ha egyáltalán képes rá… .
- Hibás és nem teljesítési kötbérek mértéke szavatoló pénzügyi helyzet elemzéssel.
- A szolgáltató menedzsment és tulajdonosi szerkezet elemzése, **mert sosem az semmi aminek elsőre látszik**…., politikai kockázat van-e? Oroszország esete.
- Titoktartási kérdések.
- Az eIDAS szempontok, ha olyan folyamat érintett, amelyben kötelezettség vállalás van, digitális aláírás/időbélyegzés/szervezeti bélyegzés.
- A Felhő és a TELKO **üzemeltetői kollegái egyedi kockázatot jelentenek-e?**
- … és sok sok lenne még, de ezeket csak akkor érdemes elemezni, ha fentiekre van jó válasz.

HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI
SZAKOSZTÁLY

Köszönöm a megtisztelő jelenlétet és figyelmet!