ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS
BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Lehet auditálni a publikus felhőket?

Oláh István doktorandusz

HTE INFOKOM 2024 Konferencia
2024. november 5.
Mátraháza, Ózon u. 1

Mi a felhő?

- Egy technológia,
- Erőforrás,
- Szolgáltatások,
- …
- A gyakorlatban sokan keverik ezeket a gondolkodásban.

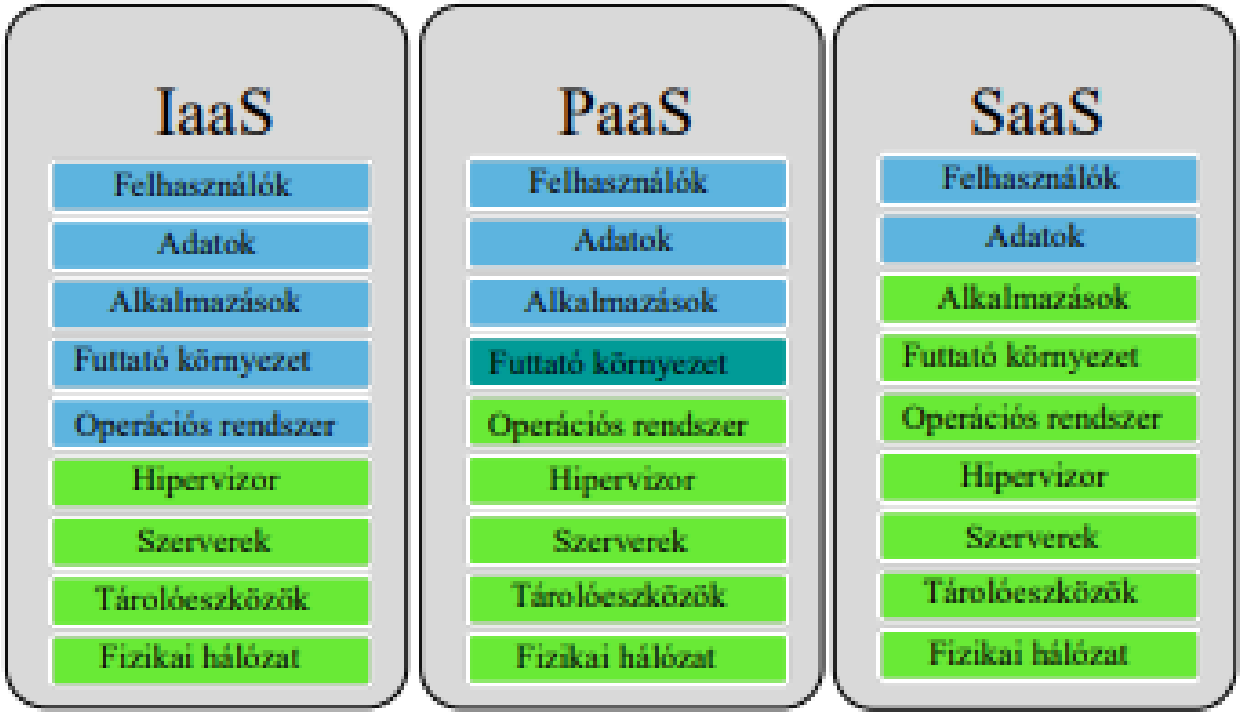
- A földön is lehet a publikus felhő! Hibrid Cloud.

Forrás: https://www.usanotebook.hu/blog/mi-az-a-felho-es-miert-jo/467

Egy publikus felhő jellemzői

- A publikus felhőszolgáltatás öt lényegi ismérve a következő NIST SP 800-145:
  - a szolgáltatás igény szerinti, akár önkiszolgáló módon való igénybevétele,
  - általános hálózati elérés,
  - megosztottan használt erőforrások,
  - a változó kapacitás-igények gyors lekövetése,
  - mért szolgáltatás (felhasználással arányos használati díj).

A publikus felhő felelősségi határai



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

Kontrollok a felhőben?

Egy adat szempontjából érdektelen, hogy:

- User hoston,
- Server hoston,
- Storageon,
- Fentiek virtuális verzión,
- Szalagon,
- Lemezen,
- Hordozható adathordozón,
- Mobil eszközön,
- …….
- A Felhőben,

Van.

A védelemnek egyenszilárdnak, és kockázatokkal arányosnak szükséges lennie!

Kutatási eredmény, az öt lépéses kontroll módszertan

Ibtv. Megfelelés kontroll szinten- I

- A bemutatott eset a Microsoft Azure plafromra értelmezett, de az öt lépés minden publikus felhőszolgálatónál elvégezhető,
- Az AzPolicyAdvertizer/semicolon lapon az Azure policydefiníciók összefoglalása található meg. Az Azure védelmi profilok egyes adatai innen kerülnek az Azureba,
- **Első lépésként** célszerű „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet kontrolljait NIST azonosítóval összerendelni, pl:

BM rendelet			MK rendelet			NIST
A munkaszakasz zárolása	3.3.10.10.	3.3.10.10.2. Képernyőtakarás: A munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel – ami a záró személy nevét is tartalmazhatja – kell eltakarni.	Eszköz zárolása, Képernyőtakarás	2.83.	Az érintett szervezet az eszköz zárolása során elrejti a kijelzőn lévő információkat. A szervezet az eszköz kijelzőjén statikus vagy dinamikus képeket jelenít meg a zárolás időtartama alatt. Az eszköz zárolása során a szervezetnek gondoskodnia kell arról, hogy a kijelzőn lévő információk ne legyenek láthatóak. Ezáltal a szervezet megakadályozza a jogosulatlan személyek számára történő hozzáférést.	AC- 11 (1)

Ibtv. Megfelelés kontroll szinten- II

- **Második lépésben** a NIST kód alapján az audit dokumentumokban megkeresni az adott kontrollt:

NIST			
AC-11 (1)	Device Lock, Pattern-hiding Displays	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

- **Harmadik lépésben** a kontrollal kapcsolatos előírás értékelése következik megfelel, vagy nem felel meg **lehetőség szinten**: IGEN!

Ibtv. Megfelelés kontroll szinten- III

- **Negyedik lépésben**, az adott kontroll kialakítását szükséges előírni egy EIR biztonsági rendszertervében,
- **Ötödik lépésben** az pl. Azure-ban az adott rendszere az érvényesítő paramétereket hangolni szükséges, azaz az alapbeállításokat kontrollonként végig kell gondolni, és a hangolást elvégezni,
- Amennyiben nem lehet közvetlen a kontrollt kialakítani, akkor kiegészítő kontrollokat szükséges előírni,
- Az előíró jellegű lépések a forráshelyről pl. excel exportot alkalmazva úgy végezhetők el könnyedén, hogy egy „üres OVI” táblába az összerendelési logikát bevisszük, azaz az ovi táblát egy felhős + *„füllel”* látjuk el.

Ibtv. Megfelelés kontroll szinten- IV

- Az adott rendszer biztonsági előírásait a kibővített „ovi” fájlban ugyanúgy lehet kezelni mint a többi kontrollt,
- Az előírt kontrollok (kiegészítő/helyettesítő kontrollok) paramétereit **nem szükséges egyenként konfigurálni,** mert a "M" (Mandatory), és az "O" (Optional) értékeket fileból be lehet olvasni, és az értékek benne lehetnek egy egy rendszer biztonsági leíró adatbázisában, akár az ovi táblájában is,
- A biztonságos környezet egyszerűen és gyorsan alakítható így ki, sőt a változásokra riasztás állítható be (Sentinel).

Kutatási eredmény, a publikus felhőszolgálató adatközpontjára az igénybevevő szervezet fizikai kontrolljait alkalmazni szükséges.

Az adatközpont szemlélet a fizikai biztonságra ?

- Egy publikus felhőszolgáltató műszaki épültei **ugyanúgy a szervezet működési fizikai tere, mint a saját épületek, saját adatközpontja a védelem szempontjából.**
- A fizikai kontroll, és az objektumbiztonsági előírásokat a szolgálatóra is érvényesíteni szükséges.
- Amennyiben ez nem lehetséges, kiegészítő kontrollt szükséges alkalmazni!

Példa egy kiegészítő kontrollra:

BM rendelet			MK rendelet			NIST
Kriptográfiai védelem	3.3.8.5.2	Kriptográfiai mechanizmusokat kell alkalmazni a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének a védelmére az ellenőrzött területeken kívüli szállítás folyamán	Adathordozók szállítása	11.6.	1. A szervezetnek biztosítania kell, hogy a digitális és analóg adathordozókat megfelelő biztonsági intézkedésekkel védje és ellenőrizze az ellenőrzött területen kívülre történő szállítás alatt. Digitális adathordozók alatt például a következőket érthetjük: lemezek, mágnesszalagok, külső/cserélhető merevlemezek, flash meghajtók, CD és DVD. Az analóg adathordozók közé tartozik például a papír és a mikrofilm. 2. A szervezetnek biztosítania kell az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás alatt. Ez magában foglalhatja a szállítási tevékenységek korlátozását az arra jogosult személyekre, valamint a szállítási tevékenységek nyomon követését. 3. A szervezetnek dokumentálnia kell az adathordozók szállításával kapcsolatos tevékenységeket. Az érintett szervezetnek rugalmasan kell meghatároznia a különböző típusú adathordozók szállításával kapcsolatos nyilvántartások módszereit, az EIR kockázatértékelése alapján.	MP-5

NIST MP-5

MEDIA TRANSPORT

- Control: The organization:
  - a. Protects and controls [Assignment: organization-defined types of information system media] during transport **outside of controlled areas using** [Assignment: organization-defined security safeguards],
  - b. Maintains accountability for information system media during transport outside of controlled areas,
  - c. Documents activities associated with the transport of information system media,
  - d. **Restricts the activities associated with the transport of information system media to authorized personnel.**

A KULCSOK a KULCS!

- Lehetőség szerint ne a szolgálató eszközein képezzük a kulcsokat, mert a maradványinformációkra is gondolni érdemes,
- A kulcsmenedzsment legyen szabályozott, zárt,
- A kulcsokhoz a felhő szolgáltató ne férjen hozzá!
- Az adatnak valahol ott kell lennie natívan! Ha máshol nem a memóriában, ezért mindent naplózni szükséges!
- HSM!
  - szoftveres ,
  - hardveres .

Forrás:
https://www.uscloud.com/azure-dedicated-hsm/

A Hol lehet a kontrollokat kialakítani?

MINDENHOL !

mert egy, egy kontroll nem szolgáltató, és/vagy technológia, és/vagy fizika tér függő!

Felhasznált Irodalom

- 2012. évi CLXVI. Törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről,
- 2013. évi L. Törvény az állami és önkormányzati szervek elektronikus információbiztonságáról,
- 2023. évi XXIII. Törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről,
- 2009. évi LXXXV. Törvény a pénzforgalmi szolgáltatás nyújtásáról,
- 2013. évi CCXXXVII. Törvény a hitelintézetekről és a pénzügyi vállalkozásokról,
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről,
- 42/2015. (III. 12.) Korm. Rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről,
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről,
- az EBA felhőszolgáltatások igénybevételével való kiszervezésre vonatkozó ajánlásai (EBA/REC/2017/03),
- **ISO/IEC 27017:2015 Code of Practice for Information Security Controls,**
- **ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud,**
- NIST Special Publication 800-145 Peter Mall és Tim Grance, „U.S. Department of Commerce , National Institute of Standards and Technology,”
- NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations,
- NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Federal Information Systems and Organizations,
- Gartner, The Cloud Strategy Cookbook, 2023, Published 1 February 2023 - ID G00776528 - 18 min read, By Analyst(s): David Smith,
- Gartner, The Future of Cloud in Banking: Vision For 2027Published 14 December 2022 - ID G00779326 -- ID G00779326 - 4 min read: Vittorio D'Orazio ittorio D'Orazio
- ENISA: Cybersecurity Certification Statistics Report, Evaluations & Certifications - State of Play 2018-2022,
- ENISA: Security Framework for Governmental Clouds February,
- ENISA: Secure Use of Cloud Computing in the Finance Sector, DECEMBER 2015, Rossen Naydenov, Dimitra Liveri, Lionel Dupre, Eftychia Chalvatzi,
- DR. BEREK LAJOS, DR. BEREK TAMÁS, BEREK LÁSZLÓ, SZEMÉLY- ÉS VAGYONBIZTONSÁG, ÓE-BGK 3071 Budapest, 2016.
- Oláh István: Hogyan érvényesülnek az Információbiztonsági kontrollok egy publikus felhőben, HÍRVILLÁM = SIGNAL BADGE 2023 pp. 81-92. , 12 p. (2023),
- Oláh István: Electronic Information Systems security –similaritires and differences on tha ground and in the public clouod HÍRVILLÁM = SIGNAL BADGE Nemzetközi Katonai Információbiztonsági Konferencia 2023-04-27 pp. 57-66. , 10 p. (2023)
- Oláh István, Magyar Sándor: Biztonsági kérdések egy publikus felhőben Magyarország :Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar (2023),
- Azure Dedicated HSM https://www.uscloud.com/azure-dedicated-hsm/,
- https://www.azadvertizer.net/index.html,
- https://www.usanotebook.hu/blog/mi-az-a-felho-es-miert-jo/467

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS
BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Köszönöm megtisztelő figyelmüket!

Óbudai Egyetem
Biztonságtudományi Doktori Iskola