**A kiszervezés egy speciális esete:**
**a felhőszolgáltatások biztonságáról**
**➔ követelményekről,**
**➔ megoldási eszközökről**

**Dr. Szenes Katalin, CISA, CISM, CGEIT, CISSP**

**Óbudai Egyetem ← BMF ← Kandó**
**Neumann János Informatikai Kar**
**szenes.katalin@nik.uni-obuda.hu**

tartalomjegyzék

- a mi Iskolánk, az Óbudai Egyetem
- a felhő remélt előnyei - idézetek a szakmai legjobb gyakorlatból
- egy szolgáltatási modell:
  a COBIT 5, és a Cloud Security Alliance anyagai alapján
- Cloud deployment model - COBIT 5
- Cloud Security Alliance Releases - latest in research

tartalomjegyzék

- a probléma egyik oldala: az én örökzöld fóliám a kiszervezéshez
- minimum követelmények egy sikeres kiszervezéshez - szerintem

- a módszertanom
  - kiválósági kritériumaim
  - alappilléreim
  - kockázat definícióm

- a módszertanom, és a felhő:
  - pillérek, kiválósági kritériumok felhő esetre, stratégiai célok szolgálatában

- a felhő specialitásaiból eredő kockázatok
  - **HF** megoldásuk módszertanom segítségével

tartalomjegyzék

- informatikai biztonsági / IT audit szempontok felhő szolgáltatáshoz

- felhő rétegek a PCI adatbiztonsági szabványa szerint

- ajánlott tevékenységek, célok az ISACA COBIT módszertana szerint
  - a rendszerbiztonsághoz - COBIT 4.1
  - a helpdeszkhez, és az incidenskezeléshez - COBIT 4.1
  - a működéshez - ISO

- irodalomjegyzék
  - saját tudományos munkáimból (PCUBE-SEC módszertan)
  - a legjobb szakmai gyakorlatok közül
    - ISACA, NIST, ISO,
    - Cloud Security Alliance,
    - PCI Security Standards Council

Kandó MSZTI ➔ Óbudai Egyetem, Neumann Informatikai Kar

1998. - Magyarországon először: Informatikai audit
2002. - Informatikai biztonság, államvizsgával
2006. - Informatikai biztonsági szakirány

mi történik a tanításon kívül? mit tudunk adni Magyarországnak?
a magyar informatikának? - olyat, amit a ***gyakorlatban*** használni lehet?

kutatást!

- szakirodalom tanulmányozása
- módszertan alkotás
- cikk-, könyvírás

példa: módszertanom használata a felhő szolgáltatások értékelésében

*Szenes* 5

a felhő remélt előnyei - idézetek a szakmai legjobb gyakorlatból

- ISACA - Information Systems Audit and Control Association
  - hatékonyabb, agilisabb vállalkozás
  - innovatívabb, versenyképesebb szolgáltatásokkal
  - kevesebb működési költséggel

"Cloud governance: questions boards of directors need to ask"
© ISACA, 2013

- NIST - USA National Institute of Standards and Technology
  - szerveridő, tárolási kapacitás automatikusan, emberi beavatkozás nélkül
  - szélessávú hálózati hozzáférés
  - erőforrás pooling - helyfüggetlen, dinamikus szolgáltatás
  - elasztikus szolgáltatás
  - mérhető, felügyelt szolgáltatás

NIST Special Publication 800-145 (Draft), 2011

*Szenes* 6.

egy szolgáltatási modell

- a COBIT 5 szerint:
  Controls and assurance in the cloud: using COBT® 5
  © 2014 ISACA.

- ebben a COBIT 5 ezt idézi:
  Cloud Security Alliance, “Trusted Cloud Reference Architecture,”
  25 February 2013,

*https://downloads.cloudsecurityalliance.org/initiatives/tci/TCI_Reference_Architecture_v2.0.*

7.

idézet a Cloud Security Alliance
“Trusted Cloud Reference Architecture” anyagából, 11. oldal
a Cloud Computing Service Delivery and Deployment Model dimenziói:

- "Cloud Trust:
  - Governance
  - Authentication
  - Auditabiity
  - Identity
  - Authorization
- Cloud Delivery:
  - Platform as a Service
  - Software as a Service
  - Infrastructure as a Service
- Cloud Operation:
  - Public
  - Hybrid
  - Private"

a dimenzió fogalmat én használom ilyen esetekben, az eredetiben nincs : szk

8.

"Cloud Deployment Model" - COBIT 5 anyag, 4. ábra alapján

- "Private Cloud
  - Operated solely for one enterprise
  - May be managed by the enterprise or a third party
  - May exist on- or off-premise
- Public Cloud
  - Made available to the general public or a large industry group
  - Owned by an organization selling cloud services
- Community Cloud
  - Shared by several enterprises
  - Supports a specific community that has a shared mission or interest
  - May be managed by the enterprises or a third party
  - May reside on- or off-premise
- Hybrid Cloud
  - A combination of two or more cloud deployment models (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability, e.g., cloud bursting for load balancing between clouds"

9.

de mi van a biztonsággal? - https://cloudsecurityalliance.org/

**Latest In Research:**

- September 25, 2014
  Survey Opportunitiy: Cloud Adoption in the Finance Industry
- September 23, 2014
  New Cloud Security Alliance Survey Reveals
  Emerging International Data Privacy Challenges
- September 18, 2014
  Cloud Security Alliance Releases New Big Data Taxonomy Report

*Szenes*

10.

a probléma egyik oldala: az én örökzöld fóliám a kiszervezéshez

mit kell *okvetlenül* tudni? - a kedvenc jelmondatom

ha akarom - vemhes
ha nem akarom - akkor is vemhes

akármit is helyezünk ki:
- feladatot
- az emberi / tárgyi erőforrásokat
- stb.

***a felelősség bent marad***

a felhő emiatt is jó példa módszertanom alkalmazására, hiszen:
- a kiszervezés egy ***működés-támogató*** folyamat

  ➔
- az intézmény ***üzleti céljaiból*** eredő szükségleteken kell, hogy alapuljon

*Szenes* 11.

minimum követelmények egy sikeres kiszervezéshez - szerintem
ld. az Informatikai biztonsági kézikönyv fejezetemet

- a belső és a külső szolgáltatók szolgáltatási szintje
  - meg van határozva?
  - felügyelt?

  - a szervezet céljait az informatikai szolgáltatások figyelembe veszik-e?
  - a kapacitás és teljesítménymonitorozási eszközök és módszerek használata
- a költségek ellenőrizhetővé tétele ≠ költségcsökkentés!

viszont javítási esély:
- ha a tevékenységekhez
  - pontosan meghatározzák
  - hozzájuk is rendelik
- a cél eléréséhez szükséges emberi / anyagi erőforrásokat

*Szenes* 12.

a könyvfejezet után pedig jöjjön a módszertan!
példa a felhő szolgáltatás értékelésének, sőt, kialakításának támogatására

- kiválósági kritériumok
  az ISACA, és az ISO információ kritériumainak kiegészítése, és általánosítása az *intézményi* működésre
  (ISO - International Standard Organization)

- a működés alappillérei
  a stratégiai célokat szolgáló célok / intézkedések azonosításának és osztályozásának támogatására

- adott célhoz és annak megvalósításához kötött kockázat fogalom:

kockázat ( cél) **~** távolság (vagyonelem, cél)
támadás bekövetkezésének valószínűsége (elem)
sérülékenység (elem)
ahol elem: a "cél" eléréséhez szükséges emberi / tárgyi erőforrás, vagyonelem

*Szenes* 13.

**kiválósági kritériumaim**

**-** *ajánlásom* konkrét, a stratégiai célok megvalósulásához *hozzájáruló* működési célokra:

↗ működési kiválósági kritériumok

↘ vagyon - erőforrás kezelési kiválósági kritériumok

*Szenes* 14

*működési kiválósági kritériumok:*

- a stratégia alapú cél- és működési kockázatkezelés kiválósága - új
- funkcionalitás - új
- rend - új
- célravezető működés - operational effectiveness
- működési hatékonyság - operational efficiency
- működési megfelelés - operational compliance
  (törvényeknek, előírásoknak való megfelelés)
- működési megbízhatóság - operational reliability

*Szenes* 15

*vagyon/ erőforrás kezelési kiválósági kritériumok:*

- működési bizalmasság - operational confidentiality
- működési sértetlenség - operational integrity
- működési rendelkezésre állás - operational availability

*Szenes* 16

mit jelent a *rend* az IT szakterület speciális esetében?

**rend**
- az IT is szolgálja saját eszközeivel az intézményi rendet,

tehát
az IT vezető
🛠 kialakítja (kialakíttatja) ***legalább*** a *következők* rendjét:
- dokumentáció,
- működési és IT üzletmenet folytonosság tervezés és kezelés,
- változáskezelés,
- konfigurációkezelés,
- incidenskezelés

🛠 be is tartatja
itt szerepet kap mind3 pillér: szervezet, szabályozás és technika

*Szenes* 17

az intéményi működés alappillérei:
a szervezet, a szabályozás, és a technika

az alappillérek rendszere = előre definiált fiókosszekrény
- intézkedési és cél típusok *ajánlására*
- a pillérek három fiók a célokról - intézkedésekről gyűjtött információnak, ahol ez releváns szempontok, pl. az intézkedések értelmezési tatománya, és értékészlete szerint *rendezve* tárolható, majd
- feldolgozáskor pedig e szempontok szerint lehet elővenni
  jól jön pl.:
  - kockázat becslésekor, majd
  - kezelésekor is

**tehát az alappillérek** ötletet adhatnak, hogy**:**
- milyen területen érvényesíthető / érvényesítendő intézkedéseket érdemes gyűjteni?
- ezek hol fognak hatni?
- a gyűjtött intézkedéseket hogy rendezzük, osztályozzuk?
- ki, miért, mikor, mit használva, ki engedélyezi, ki ellenőrzi...

*Szenes* 18.

a probléma másik oldala

visszatérés a felhőkhöz

19.

pillérek / kiválósági kritériumok felhő esetre

stratégiai cél ← üzleti cél

- azonnali rugalmasság - igény szerinti rendelkezésre állás
- erőforrások összpontosítása - hatékonyság

de: probléma lehet az adatforrás - cél közti távolság, ha felhőbe tesszük át:
- a VOIP telefonszolgáltatást, vagy
- kismennyiségű adatok gyakori mozgatását, pl. mail, archiválás szolgáltatás

keressünk tehát javító (preventive, detective) intézkedéseket:
- szervezeti - kinevezés:
  - üzleti szakterületi felelőst, aki jelzi, ha probléma van,
  - hálózati adminisztrátor, aki
- beállítja a quality of service-t - technikai

*Szenes*

20.

példa - pillérek / kiválósági kritériumok stratégiai célok szolgálatában

stratégiai cél:
védekezés a belső támadások ellen,
ehhez legyenek részcélok ezek a kiválósági kritériumok:

- rend
- bizalmasság

szabályozási aztán szervezeti intézkedés
- elrendelni, aztán végrehajtani:

- kötelességelhatárolás szabályozása, majd eszerint
- munkaköri leírás összeállítása szerepkörökből
- a szerepkörökhöz pont a szükséges jogosultságok kérése

**. / .**

*Szenes* 21.

példa - pillérek / kiválósági kritériumok stratégiai célok szolgálatában

szabályozási, majd technikai intézkedés:

- jogosultságok engedélyeztetése, majd beállítása
- a már szükségtelenek visszavonása

jogosultság-, és egyéb kérések intézményi kezelésének folyamatát
***meg kell szervezni***

kérelmező ↗ adat- / üzleti folyamat tulajdonos ↘ biztonsági szakterület
↖ ↙
technikus, aki beállítja

*Szenes* 22.

a felhő specialitásaiból eredő kockázatok
[irodalom: Vohradsky; könyvfejezetem a kiszervezésről a z Informatikai buatinségi nn ]
- HF megoldásuk a kritériumok, pillérek segítségével?

- bűnözők kihasználják a névtelenséget
- nem biztonságosak az interface-k
  - névtelen hozzáférés
  - titkosítatlan autentikációs adatok, adatátvitel
- a cloud szolgáltató belülről - belső rosszindulat **! [**rendetlenség**]**
  - az emberi erőforrás
  - biztonsági problémák, incidensek kezelése
  - válalati üzleti folyamataik felügyelete és irányítása (supply chain)

23.

a felhő specialitásaiból eredő kockázatok
[Vohradsky és kiszervezés könyvfejezetem]
- HF megoldásuk a kritériumok, pillérek segítségével?

- egyik felhasználó a másik ellen
- az adatkezelés elszámoltathatósága
  - tulajdonlás
  - törlés
  - rendelkezésre állás
  - átvitel, titkosítás
  - működési hibák, stb.
- eltérítés
  - felhasználót
  - szolgáltatást

  megtévesztéssel, csalással, sérülékenységek kihasználásával

24.

a felhő specialitásaiból eredő kockázatok
[Vohradsky és kiszervezés könyvfejezetem]
- HF megoldásuk a kritériumok, pillérek segítségével?

- átláthatatlanság (a résztvevő felek közt)
  - különféle országok előírásai szerinti szabálykövetés
    - adatvédelem, stb.
  - biztonsági eljárások, pl. monitorozás, naplózás
  - rend, úgymint pl. konfigurációkezelés - stb. ld. a kritériumaimat
- a felhasználók kezelése
- a vevő elkötelezettsége **?** hordozhatóság
- üzletmenet folytonosság
  - szolgáltatás közbeni probémák - ***kinek*** a problémáit tudjuk kezelni?
- felhasználói tevékenységekből
  - lehetőségek felhasználási módjából eredő problémák,
  - a vevő fejlesztési, tesztelési szokásaiból, szabályaiból

***de mindez csak részleges segítség !*** pl. vírus a hypervisorban

25.

informatikai biztonsági / IT audit szempontok felhő szolgáltatáshoz

↗ vevői követelmények miatt, pl.
- szakágazat szerint, vagy
- stratégiai célok miatt,
- stb.

➔ a szolgáltatás jellegével kapcsolatos követelmények
- egy lehetséges osztályozás:
Software, Platform, Infrastructure, Security aaS

↘ érzékenység / biztonsági tartomány szerint:
hálózat - adatátvitel, adattárolás, szolgáltatás
(Chen, Wang, Wang: On-demand Security Architecture for Cloud Computing
Computer, July 2012, IEEE Computer Society, p. 73-78)

ezekhez a dimenziókhoz hozzárendelhetőek a kiválósági kritériumok,
akár üzleti célok szerint súlyozva is

*Szenes*

26.

informatikai biztonsági / IT audit szempontok felhő szolgáltatáshoz
példa:
mátrix a PCI adatbiztonsági szabványa szerint

- sorok:
  felhő réteg
- oszlopok:
  szolgáltatási modell
- mátrixelemben jelezzük:
  kié a felelősség - a vevőé? a szállítóé? mindkettőé? - ***vagy?***

***PCI Security Standards Council:***
***Standard: PCI Data Security Standard (PCI DSS)***
Version: 2.0 Date: February 2013
Author: Cloud Special Interest Group PCI Security Standards Council
Information Supplement: PCI DSS Cloud Computing Guidelines
https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

*Szenes* 27.

felhő rétegek a PCI adatbiztonsági szabványa szerint

- Adatok
- Interfészek (API-k, GUI-k)
- Alkalmazások
- Megoldási stack - Programnyelveknél
- Operációs rendszerek
- Virtuális gépek
- Virtuális hálózati infrastruktúra
- Hypervisorok
- Processing és memória
- Adattárolás (merev-, cserélhető lemezek, backup-ok, stb.)
- Hálózatok (interfészek és eszközök, kommunikációs infrastruktúra)
- maguk a fizikai Telephelyek / adatközpontok

*Szenes* 28.

ajánlott tevékenységek, célok az ISACA COBIT módszertana szerint
a rendszerbiztonsághoz - COBIT 4.1

DS5.1 Az IT biztonság irányítása

- DS5.2 IT biztonsági terv
- DS5.3 Identity Management
- DS5.4 User Account Management
- DS5.5 A biztonság tesztelése, felülvizsgálata, és felügyelete
- DS5.6 A biztonsági incidens definiálása
- DS5.7 A biztonságot szolgáló technika védelme
- DS5.8 A titkosítási kulcsok kezelése
- DS5.9 A rosszindulatú programok felderítése, működésük megakadályozása, hatásuk javítása
- DS5.10 Hálózatbiztonság
- DS5.11 érzékeny adatok mozgatása

(***COBIT*** ® 4.1 Framework, Management Guidelines, Maturity Models
Copyright © IT Governance Institute®, 2007
- saját magyar nyelvű értelmezés)

*Szenes* 29

ajánlott tevékenységek, célok az ISACA COBIT módszertana szerint
a helpdeszkhez, és az incidenskezeléshez - COBIT 4.1

DS8 A helpdesk és az incidensek kezelése

- DS8.1 Szolgáltató deszk felállítása, és működtetése
- DS8.2 Az ügyfelek kéréseinek regisztrálása
- DS8.3 Az incidensek eszkalációja
- DS8.4 Az incidensek lezárása
- DS8.5 Jelentések és trendvizsgálatok

(***COBIT*** ® 4.1
Framework, Management Guidelines, Maturity Models
Copyright © IT Governance Institute®, 2007
- saját magyar nyelvű értelmezés)

*Szenes* 30

ajánlott tevékenységek, célok az ISACA COBIT módszertana szerint a helpdeszkhez, és az incidenskezeléshez - COBIT 5

"DSS01.02 A kiszervezett informatikai folyamatok irányítása
Úgy kell irányítani a kiszervezett IT szolgáltatások működését, hogy

- az intézmény információinak védelme fennmaradjon
- a szolgáltatás biztosítása megbízható legyen."

ajánlott "tevékenységek":

- **...**informatikai folyamatok biztonsága **...**
- **...** a szolgáltatási szerződések, SLA-k az üzleti és IT követelményekkel összhangban **...**
- **...** a vevő és a szállító integrálja kritikus IT irányítási folyamatait **...**
- **...** a szolgáltató **...** auditálása, a követelmények teljesítése érdekében **...**

(**COBIT** ® 5: Enabling Processes
Copyright © 2012 ISACA., ISBN 978-1-60420-241-0)

*Szenes* 31

ajánlott tevékenységek, célok a működéshez - International Standard Organization

a 27001-es szabvány függelékéből:
8 Működés
8.1 A működés tervezése és ellenőrzése

**...** a szervezetnek biztosítania kell, hogy meghatározzák a kiszervezett folyamatokat, és ellenőrizzék ezeket**...**

International Standard ISO/IEC 27001
First edition 2005-10-15
International Standard ISO/IEC 27002 First edition 2005-06-15
Information technology — Security techniques — Code of practice for information security management

jelenlegi kiadásuk: 2013-as

*Szenes* 32

irodalomjegyzék - saját tudományos munkáimból
(PCUBE-SEC módszertan)

- felhasználható fejezetek *kézikönyvekből*
  **a felhő a kiszervezés egy speciális esete**
  ⬇
  Szenes, K.: Az informatikai erőforrás-kihelyezés auditálási szempontja
  Az Informatikai biztonság kézikönyve, Verlag Dashöfer, Budapest, I.-II. rész

- felhasználható ötletek *módszertanból*
  Szenes Katalin: Informatikai biztonsági módszerek kiterjesztése a vállalatirányítás, a működés, és a kockázatkezelés támogatására
  Minőség és Megbízhatóság folyóirat, kiadó: Dr. Molnár Pál elnök,
  European Organization for Quality (EOQ)

  K. Szenes: Operational Security - Security Based Corporate Governance
  Procds. of IEEE 9th International Conference on Computational Cybernetics
  July 8-10, 2013 Tihany, Hungary @2013 by IEEE

irodalomjegyzék - a legjobb szakmai gyakorlatok közül - ISACA

- COBIT® 4.0 Control Objectives, Management Guidelines, Maturity Models
  Copyright © IT Governance Institute® , 2005, editor: ISACA

- COBIT® 4.1 Framework, Management Guidelines, Maturity Models
  Copyright © IT Governance Institute® , 2007, editor: ISACA

- "Cloud governance: questions boards of directors need to ask"
  © ISACA, 2013

- Controls and assurance in the cloud: using COBT® 5
  © 2014 ISACA.

- COBIT ® 5: Enabling Processes
  Copyright © 2012 ISACA., ISBN 978-1-60420-241-0)

- David Vohradsky: Cloud Risk—10 Principles and a Framework for Assessment
  ISACA Journal Vol. 5, 2012, © 2012, ISACA, editor: ISACA

irodalomjegyzék - a legjobb szakmai gyakorlatok közül,
NIST, ISO, Cloud Security Alliance

- NIST Special Publication 800-145 (Draft), 2011
  W. Jansen, T. Grance: Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology, January, 2011

- Cloud Security Alliance, “Trusted Cloud Reference Architecture,”
  25 February 2013,

*https://downloads.cloudsecurityalliance.org/initiatives/tci/TCI_Reference_Architecture_v2.0*.

- International Standard Organization
  - az említett ISO/IEC 27001 és 27002
  - a 27000-es biztonsági család többi tagja: 27005, 27000

- mm

irodalomjegyzék - a legjobb szakmai gyakorlatok közül
PCI Security Standards Council

- ***PCI Security Standards Council:***
  ***Standard: PCI Data Security Standard (PCI DSS)***
  Version: 2.0 Date: February 2013
  Author: Cloud Special Interest Group PCI Security Standards Council
  Information Supplement: PCI DSS Cloud Computing Guidelines

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

36.

references - publication


- Chen, Wang, Wang: On-demand Security Architecture for Cloud Computing Computer, July 2012, IEEE Computer Society, p. 73-78