A szoftverszolgáltatások kockázatai üzleti szemmel - DRAFT

Horváth Csaba

PwC Magyarország

pwc

A szoftverszolgáltatások növekvő kockázatai

- 2011. április adatvesztés az AWS EC2 szolgáltatásban
- A kibertámadások folyamatosan növekvő száma: 2012-ben 42 %-os növekedés az előző évhez képest*
- Kötelező szabályozási és kontroll megfelelősség magas kockázattal járó adatok esetén (személyes, pénzügyi stb.)

Kibertámadási példa

A Sony Playstation játékkonzol hálózatának meghackelését követően **70 millió előfizető személyes, hitelkártya és egyéb adat**ait lopták el, mely **23 napig volt hatással a hálózat elérhetőségére**, ezáltal **171 millió USD-s veszteség**et okozva a cégnek

A felhőszolgáltatások egyedi kockázatai

- felhőszolgáltatók bizonytalan képessége a biztonsági szabályzatok betartatásával kapcsolatban
- esetleges nem megfelelő képzés és IT audit
- megkérdőjelezhető kontroll a kiemelt hozzáférések felett a szolgáltató telephelyén
- az adatvisszatöltéssel kapcsolatos bizonytalanság
- a vállalati adatok egyéb vállalatokhoz való közelsége
- a szolgáltató auditálhatóságának bizonytalansága
- a pay-as-you-go számlázási modell átláthatósága és jogossága

Kockázattudatosság

A kockázatokra válaszként megjelent a rálátásigénye a szolgáltatói oldalon megvalósuló:

- privacy-ra,
- teljességre,
- biztonságra és
- információelérhetőségre.

Felelősség kérdése

Attól függetlenül, hogy egy cég:

- továbbra is cégen belül valósítja meg az IT-t,
- hagyományos kiszervezett szolgáltatást vesz igénybe,
- magán, publikus vagy hibrid felhőszolgáltatást használ,

az IT kormányzással, biztonsággal, elérhetőséggel, privacy-val, működési és törvényi szabályozásoknak való megfelelőséggel kapcsolatos kockázatok kezelése továbbra is a **menedzsment felelőssége** marad.

Ezen felül a menedzsment felelőssége megbizonyosodni:

- a folyamatok hatékonyságáról,
- a teljesítmény és stabilitás eléréséről
- és a törvényi és szerződésben foglalt szabályozásoknak való megfelelőségről.

- Gyakran feltett kérdések (FAQk)
- Rendszerleírások
- Kontroll leírások

Kielégítő válaszadás garanciájának hiánya

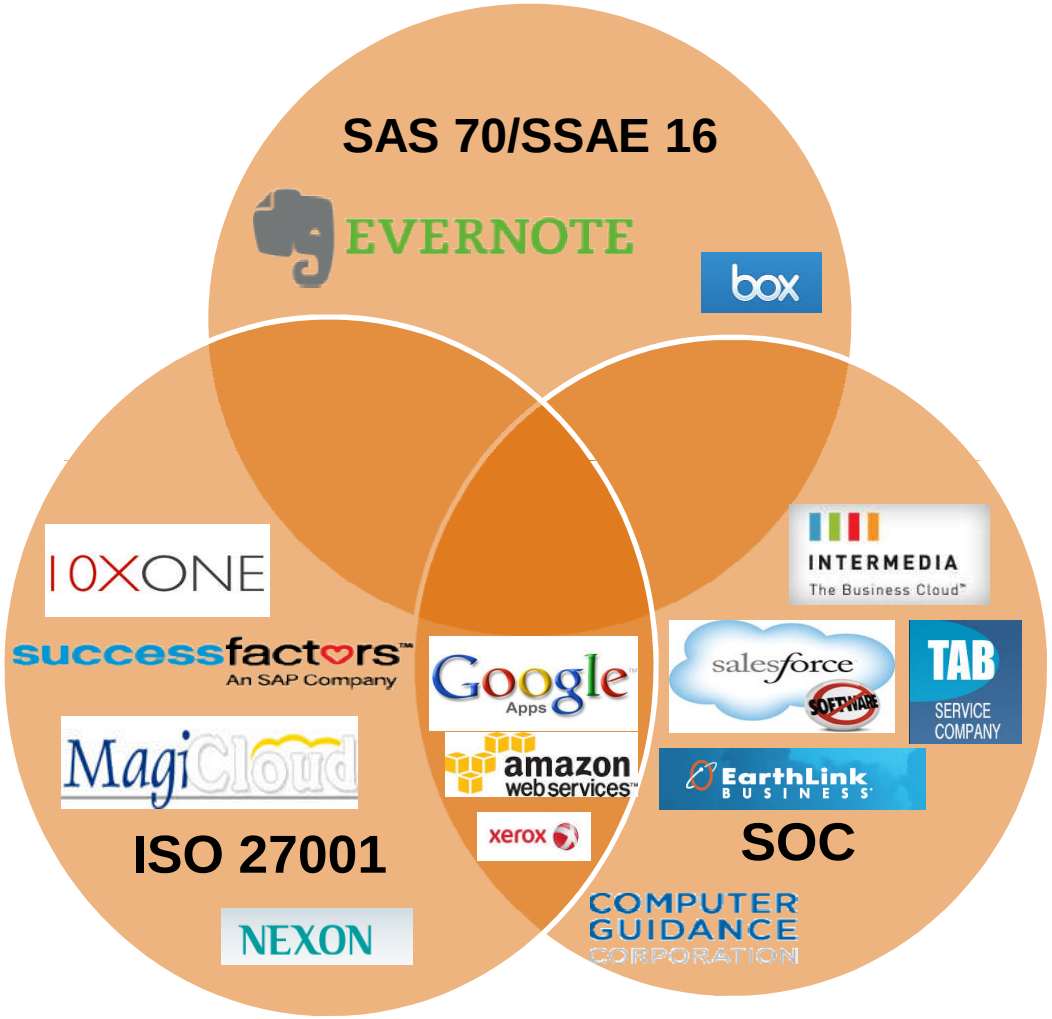
Összehasonlíthatóság problematikája

Third Party Assurance (TPA)

Third Party Assurance (TPA)

- SAS 70
- SSAE 16
- ISAE 3402
- ISO 27001
- SOC 1
- SOC 2
- SOC 3

Felhőszolgáltatók tanúsítványai



SOC 1

SAS 70-et felváltó **pénzügyi audit fókuszú riport** adott időintervallumra

Tartalma:

- Rendszerek és kapcsolódó kontrollok leírása (MÁ)
- Kontrollcélok eléréséhez szükséges megfelelősség (MÁ)
- Kontrollok működési hatékonysága (MÁ)
- CPA vélemény a menedzsment állításairól
- CPA által végzett tesztek leírása és eredményei

Célközönség: a **felhasználó cég pénzügyi menedzsment**je, **felhasználó cég auditor**ai

SOC 2

Felhőszolgáltatásokhoz kialakított **riport** adott időintervallumra

Tartalma:

- SOC 1-el megegyező
- Kivétel a fókusz, mivel ez Trust Service Principle-kre épül:
  - biztonság
  - elérhetőség
  - feldolgozás integritása
  - bizalmasság
  - privacy

Célcsoport: **vásárlók**, **szabályozók** és **üzleti partnerek**, akik egy **részletes áttekintést** szeretnének kapni a szolgáltatást nyújtó belső kontrollkörnyezetéről

Biztonság

A rendszer védett legyen az illetéktelen logikai és fizikai hozzáférésekkel szemben:

- IT biztonsági policy,
- biztonságtudatossági képzés,
- logikai hozzáférés,
- fizikai hozzáférés,
- biztonsági monitorozás,
- felhasználói autentikációs beállítások,
- eszköz klasszifikáció és menedzsment,
- konfigurációmenedzsment és változásmenedzsment

Elérhetőség

A rendszerrel kapcsolatos felhasználó és szolgáltató közötti megállapodásban lefektetett elérhetőség:

- helyreállítási célidő,
- elérhetőségi policy,
- mentés és megőrzési policy,
- katasztrófa helyreállítási terv
- és üzletmenet folytonosság menedzsment.

Feldolgozás integritása

A jóváhagyott tranzakciók időben, hiánytalanul és pontosan kerülnek végrehajtásra:

- feldolgozás integritását figyelő policy-k,
- pontossági ellenőrzések (pl. ciklikus redundancia ellenőrzés),
- nyomon követés, számlázás,
- Időbeliség,
- jóváhagyás (pl. funkcionális visszaigazolások)
- és a bemenetek pontossága.

Bizalmasság

A rendszer oly módon lett megtervezve, hogy megfelelő biztosítékkal rendelkezzen az érzékeny információk kiszivárogtatás ellen:

- bizalmassági policy-k,
- be- és kimenetek bizalmassága,
- adatfeldolgozás
- és információs beszámolók.

Privacy

A rendszer által gyűjtött, felhasznált, mentett és közzétett személyes információk a szolgáltató vállalat privacy policy-je és az AICPA privacy alapelvei szerint történik:

- privacy policy-t,
- gyűjtési folyamatot,
- adatfelhasználást és tárolást,
- Adathozzáférést,
- információ kiszolgáltatást
- és privacy megfigyelést.

SOC 3

Auditálatlan kontroll megfelelőségi és működési riport, a szolgáltató szervezet hatékony rendszerkontrolljainak karbantartásáról

Tartalma:

- SOC 2-höz hasonló
- Kivétel, hogy a kiadáshoz nem szükséges:
  - a menedzsment által meghatározott állítások
  - hozzájuk kapcsolódó audit vélemény
  - Hozzáférhető a publikum számára

Célcsoport: **bárki** aki egy **részletektől mentes átfogó kép**et szeretnének kapni a szolgáltatást nyújtó belső kontrollkörnyezetéről a bizalom megteremtéséhez

TPA költségei

Költségviselők

- SAS 70
  - Alap audit procedúrák esetén szolgáltatást nyújtócégek
  - Kiegészítő audit procedúrák esetén felhasználók
- SOC 1, 2
  - Alap audit procedúrák esetén szolgáltatást nyújtócégek
  - Kiegészítő audit procedúrák esetén felhasználók
- SOC 3
  - Összes költség a szolgáltatást nyújtócégeket terheli

Összefoglalás

A szoftverszolgáltatásokkal kapcsolatos **incidensek és növekvő fenyegetettségek** révén egyre inkább a figyelem középpontjába kerültek a velük kapcsolatos **általános és egyedi kockázatok** és azok igénybevétel előtti **értékelés**ére.

A **kezdeti tökéletlen megoldások** után (**SAS 70, SSAE 16, ISAE 3402**) került kidolgozásra a **SOC riportok keretrendszere**, mely immáron **a felhőszolgáltatások összes kritériumát figyelembe véve**:

- összehasonlítható módon képes információt szolgáltatni :
- a szolgáltatók rendszereink és kontrolljainak leírásáról,
- a kontrollcélok eléréséhez szükséges megfelelősségről,
- a kontrollok működési hatékonyságáról,
- és CPA által véleményezve a menedzsment állításait és tartalmazva a CPA által végzett tesztek leírásait és eredményeit.

Köszönöm a figyelmet és várom a kérdéseket!