Máté István Zsolt
Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola
mate.istvan@informatikaiszakerto.hu

FELHŐSZOLGÁLTATÁSOK – A KIBERBIZTONSÁGTÓL A SZAKÉRTŐI BIZONYÍTÁSIG

– előadásvázlat –

Absztrakt

A felhőszolgáltatások terjedése és különösen annak tömegesedő igénybevétele alapvető biztonsági kérdéseket vet fel. Ezek között a legnagyobb publicitást a kibertámadások kapják, ugyanakkor nem hagyhatjuk figyelmen kívül a terület kriminalisztikai vonatkozásait sem. A felhőszolgáltatások ellen, azok felhasználásával, vagy érintettségével elkövetett bűncselekmények szakértői vizsgálata és a büntetőeljárás kereti közötti szakértői bizonyítás új kihívást jelent az igazságügyi informatikai szakértőknek. A Digital Forensic Science hagyományos, részben szabványosított módszerei, eljárásai és alkalmazott eszközrendszere kiegészítést, módosítást kíván. Az előadás sorra veszi azokat az elemeket, melyekre a szakértőknek válaszokat kell adniuk a felhőszolgáltatásokkal kapcsolatos ügyek vizsgálatakor.

Kulcsszavak: *felhő, cloud, облако, forensic IT expert, судебно-информатический эксперт*

A felhőszolgáltatások fogalma

A felhő koncepciója szerint az informatika kapacitások (legyenek azok bármifélék is) olyan szolgáltatásként kell nyújtani, mint a közművek szolgáltatják a vizet, az elektromos energiát, a gázt és még néhány további alapszolgáltatást.

Ezek a rendszer a szolgáltatás típusa szerinti megközelítés alapján 3+1 fő kategóriába sorolhat, melyek a következők:

- **Software as a Service (SaaS)** >> a szolgáltató alkalmazásai használata
- **Platform as a Service (PaaS)** >> ügyfél alkalmazásainak futtása
- **Infrastructure as a Service (IaaS)** >> számítási, tárolási hálózati és egyéb kapacitások és erőforrások bérlése
- **Storage as a Service (StaaS) >>** tárhely szolháltatás (mely besorolható ugyan az IaaS szolgáltatások közé, de elterjedtségéből adódóan külön is tárgyalható)

A rendszerek informatikai oldalról egy fizikai infrastruktúrára épülő virtualizált környezetben megjelenő valós idejű szolgáltatásként foghatók fel, mely lényeges különbségeket mutat a Digital Forensic Science vizsgálati tárgyához a számítógéphez, vagy adattárolóhoz képest. (Reilly et al.)

A digitális bizonyíték

A büntetőeljárásról szóló 1998. évi XIX. törvény (Be.) szerint a bizonyítás eszközei a következők:

„76. § (1) A bizonyítás eszközei a tanúvallomás, a szakvélemény, a tárgyi bizonyítási eszköz, az okirat és a terhelt vallomása.”

Az informatikai tartalmak ezek közül (különös módon) a tárgyi bizonyíték kategóriába tartoznak, elletve közvetett módon megjelenek a szakvéleménynél is. A tárgyi bizonyítékról így fogalmaz a Be.:

„115. § (1) Tárgyi bizonyítási eszköz minden olyan tárgy (dolog), amely a bizonyítandó tény bizonyítására alkalmas, … az elkövető nyomait hordozza, vagy a bűncselekmény elkövetése útján jött létre, amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy amelyre a bűncselekményt elkövették.”
Az informatikai bizonyítékok fentieknél pontosabb definíciója az International Organization on Computer Evidence (IOCE) megfogalmazásában vált ismertté az alábbiak szerint:

> ***Digital Evidence*** – Information stored or transmitted in **binary form** that may be relied upon in court.
> ***Original Digital Evidence*** – **Physical items** and those data objects, which are associated with those items at the time of seizure.
> ***Duplicate Digital Evidence*** – A duplicate is an **accurate digital reproduction of all data** objects contained on the original physical item.
> ***Copy*** – A copy is an **accurate reproduction of information** contained in the data objects **independent of the original physical item**

Amint az kiolvasható a meghatározásokból, a digitális bizonyíték statikus adatként jelenik meg, melyet egy fizikai tárgy tárol (original physical item). A felhőszolgáltatásokban megjelenő digitális bizonyítékok jellemzően dinamikus digitális tartalmak (események, folyamatok, adatok változása), melyek a network forensic és a mobile forensic területéhez állnak közelebb, ahol a számítógépes hálózati forgalom, illetve a mobiltelefon készülékek kapcsolódási adatinak elemzése álla a vizsgálat középpontjában.
A dinamikus digitális bizonyíték (dynamic digital evidence) fogalmának megalkotásakor az előzőek miatt különös fontosságra tesz szert a dinamikus jellemzőt leíró időbélyeg (timestamp), illetve annak hitelessége és pontossága.

A Cloud Forensic módszertani jellemzői

A felhőszolgáltatásokkal kapcsolatos forenzikus vizsgálatok módszertani meghatározása már szabványosított computer forensic követelményeivel összehasonlítva történhet meg a legegyszerűbben. A vonatkozó nemzetközi szabvány a ISO/IEC 27037:2012, Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence (Információtechnológia - Biztonsági eljárások – Segédlet a digitális bizonyítékok azonosításához, összegyűjtéséhez, kinyeréséhez és megőrzéséhez).

A két terület követelmény és eljárásrendszere az Incident Management and Forensics Working Group 2013-as tanulmánya alapján a következőkben foglalhatók össze:

Követelmény	Computer Forensic	Cloud Forensic
Ellenőrizhetőség (Auditable)	Az intézkedések pontos dokumentálása a végrehajtók részéről	A dinamikus, elosztott és komplex rendszerben nehezebben teljesíthető követelmény
Megismételhetőség (Repeatable)	Azonos vizsgálati feltételek mellett azonos eredmények. – azonos mérési eljárások és módszerek – azonos eszközök használata, azonos körülmények között – - az eredeti vizsgálat tetszés szerint időben történő megismételhetősége	A dinamikus, elosztott és komplex rendszerben az „azonos feltételek” és a „bármikor az eredeti vizsgálat után megismételhetőség” követelménye nem minden esetben teljesíthető. A jelenlegi legjobb megoldás a pillanatkép módszer (snapshot forensics) > hasonlóan a futó alak állóképek sorozatával történő leképezéséhez
Reprodukálhatóság (Reproducible)	Azonos vizsgálati feltételek mellett azonos eredmények. – azonos mérési eljárások és módszerek – különböző eszközök használata, különböző körülmények között - az eredeti vizsgálat tetszés szerint időben történő megismételhetősége	
Igazolhatóság (Justifiability)	A vizsgálatot végző szakértőnek kell igazolnia az elvégzett műveleteket és a használt módszereteket	Azonos követelmény

	Computer Forensic	Cloud Forensic
Azonosítás (Identification)	– A bizonyítékok változékonyságának (volatily) figyelembe vétele a begyűjtési sorrend kialakításánál – A potenciális bizonyítékok károsodásának minimalizálása – Rejtett bizonyítékok azonosítása	– Saas - alkalmazás szintű naplófájlok – felhasználói engedély hibák, felhasználói fiókkezelési hibák (ki, mit, mikor tett), sebességproblémák ... – PaaS – programspecifikus naplófájlok, javítócsomag állapotok, hitelesítési hibák, OS kivételek és figyelmeztetések, rosszindulatú programok elleni rendszerek figyelmeztetései – IaaS – rendszer szintű naplófájlok, hypervisor rendszerek eseményei és naplóállományai, virtuális gépek nyers (raw) állományai, memóriatartalom pillanatképek, behatolás érzékelők és tűzfalak eseményei, hálózati események és hálózati adatcsomag megfigyelés, tárlók naplóállományai, mentések
Összegyűjtés (Collection)	Az összegyűjtés során a digitális bizonyítékot tartalmazó eszközt eltávolítják eredeti helyéről, laboratóriumban ellenőrzött körülmények között történő későbbi kinyerés és elemzés céljából	A felhőszolgáltatások esetén több felhasználó (szervezet) osztozik a hardver és szoftver erőforrásokon, ezért kerülni kell a fizikai eltávolítást. A művelet gyakran csak a Cloud Service Provider (Felhőszolgáltató) által végezhető el.
Kinyerés (Acquisition)	A kinyerés során másolat készül a lehetséges digitális bizonyítékot tartalmazó eszköz tartalmáról	A kinyerésnek – a felhőszolgáltatások jellegéből adódóan – a logikai elemekre kell koncentrálnia, nem a fizikai tárakra
Megőrzés (Preservation)	A megőrzés a lehetséges digitális bizonyítékok integritásának megőrzésére terjed ki, melynek során megvédjük az illetéktelen hozzáféréstől vagy eltüntetéstől.	A követelmények azonosak, azzal a megjegyzéssel, hogy a felügyeleti lánc (chain of custody) fenntartása a különböző földrajzi és jogi környezeten keresztül nem egyszerű feladat.

(IMFWG, 2013. pp.13-17)

Összefoglalás

A felhőszolgáltatások felhasználásával, az ellen, vagy annak érintettségével elkövetett bűncselekmények igazságügyi informatikai szakértői vizsgálata és a szakértői bizonyítás módszertana és eszközrendszere kialakulófélben van. A létrejövő rendszer alapját computer forensic és a network forensic eljárások és a velük kapcsolatban kialakított nemzetközi szabványok (ISO 27000 szabványkör) képezik.

A vizsgálati terület különbözőségeiből fakadó eltérések meghatározása és kezelése, figyelemmel a felhőszolgáltatások informatikai környezetére, valamint a különböző jogrendszerek egyidejű érintettségére, az igazságügyi informatikai szakértők és az érintett jogterületek és jogrendszerek szakértőinak közös feladata. A területre vonatkozó gyakorlati megoldások a szakértők és a nyomozó hatóságok (law enforcement) szoros együttműködését igénylik.

A felhőszolgáltatásokat érintő igazságügyi informatikai szakértői vizsgálati eljárások gyakorlati vonatkozásairól az előadás második részében lesz szó, mely 2014.11.20-án a Rendészeti Doktoranduszok VI: Országos Találkozóján hangzik majd el.

Irodalom

1) **Incident Management and Forensics Working Group**. 2013. Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing.
2) **Reilly et al.** Cloud Computing: Pros and Cons for Computer Forensic Investigations. in International Journal Multimedia and Image Processing (IJMIP), Volume 1, Issue 1, March 2011.
3) **Dykstra – Riehl**. Forensic collection of electronic evidence from Infrastructure-as-a-service cloud computing. in Richmond Journal of Law & Technology Volume XIX, Issue 1.
4) **Dykstra – Sherman**. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. in Digital Investigation 9 (2012) S90–S98.
5) **Ruan et al**. Cloud Forensics. In Advances in digital forensics VII. Springer Berlin Heidelberg, 2011. 35-46.
6) **Mark Taylor et al.** Forensic investigation of cloud computing systems. In Network Security March 2011.