(HELYI) HÁLÓZATOK AKTUÁLIS BIZTONSÁGI PROBLÉMÁI

SECURITY PROBLEMS OF (LOCAL) NETWORKS

Wagner György[*]*, Tóth Tibor*[**]

ABSTRACT

The use of cloud computing in Hungary is becoming more prevalent. Companies may face several security problems when partially or fully introducing this technology. Their data, their systems and also their internal policies should therefore be reviewed and modified if necessary. The paper discusses the concept of clouds, their variants and security issues concerning their use.

1. BEVEZETÉS

A számítási felhők használata Magyarországon is egyre jobban terjed. A vállalatok ezek részleges vagy teljes bevezetésekor többféle biztonsági problémával kerülhetnek szembe. Adataikat, rendszereiket, belső szabályzatukat ennek megfelelően érdemes felülvizsgálni, szükség esetén módosítani. A cikk kitér a felhők fogalmára, változataira, biztonsági kérdésekre.

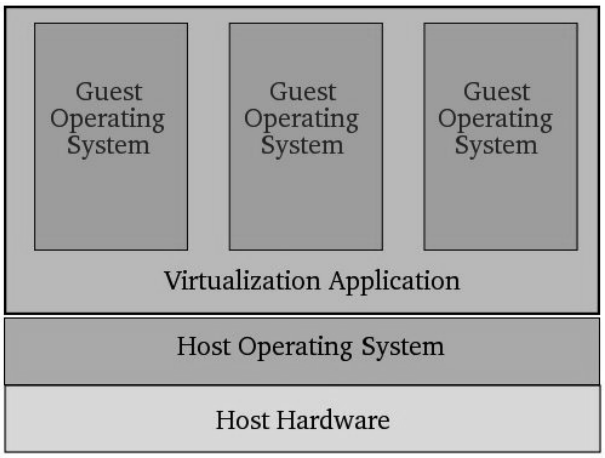
2. ELŐZMÉNYEK

Az informatikai eszközök kialakulásuk óta folyamatosan jelentős változáson estek át. Ez a Moore-nak tulajdonított (1965-ös tapasztalati) törvénynek köszönhetően (egyszerűsítve: az integrált áramkörök összetettsége 18 havonta megduplázódik) jól ismert, és elfogadott [1]. A számítógépeket kezdetben szigorúan zárt, klimatizált termekbe telepítették, sokszor csak pormentes ruhákban és csak kiképzett személyzet részére voltak közvetlenül elérhetők. Elfogadott volt a kötegelt (batch) program futtatás, amelyek a kor fejlettségének megfelelően valamilyen lyukkártyás – lyukszalagos adatbeviteli– és kiviteli eszközöket használtak. A batch alapú rendszerek a hatékony programfejlesztést, a gyors hibakeresést erősen korlátozták. Az igényeknek megfelelően először az interaktív operációs rendszerek jelentek meg, majd a személyi számítógépek kifejlesztésének, és elterjedésének köszönhetően bekövetkezett a számítóközpontok előnyökkel és hátrányokkal együttjáró decentralizációja. Felismerték, hogy a személyi számítógépek számítási kapacítása (többek között az alkalmazott architektúrának is köszönhetően) jóval kisebb, mint egy specializált rendszeré. Emiatt kifejlesztésre kerültek, és elterjedtek a fejlettebb, költségesebb architektúrájú szerver feladatokat ellátó számítógépek. A felhasználók számára kifejlesztett szoftverek ehhez illeszkedve szintén két részből tevődtek össze (két rétegűek voltak). Az egyik komponens a szerveren futott, a másik a felhasználó (kliens) számítógépén. A szoftverek idővel tovább rétegződtek annak érdekében, hogy az egyes feladatokat megvalósító részmegoldások könnyebben cserélhetők legyenek.

Az idő múlásával az asztalai számítógépek számítási teljesítménye jelentős mértékben megnőtt. Ennek kihasználására egy számítógépre több szerver szoftver is telepítésre került. Az egyes szoftvereket kiadásuk után a gyártók folyamatosan tesztelték, javították, majd a javítást (patch) valamilyen formában hozzáférhetővé tették. A patch telepítése után a számítógépet sok esetben újra kellett indítani. Az újraindítás azonban azokra a szerver funkciót biztosító rendszereket is leállította, majd elindította, amelyek nem voltak érintettek a frissítésben. (Előfordulhatott, hogy ugyanazon a számítógépen futott egy SQL szerver és egy Web szerver. Ha az SQL szerverre megjelent egy patch, aminek telepítése után a számítógép újraindításra került, akkor ez idő alatt a Web szerver sem volt elérhető).

A virtualizációs technika kifejlesztésével lehetőség nyílt arra, hogy egy fizikai számítógépen több virtuális számítógépet lehessen emulálni. A virtuális gépekre egymástól független operációs rendszereket lehetett telepíteni, majd arra a szerver feladatot ellátó szoftvert. Így minden egyes virtuális gépen csak az adott szerver funkciót biztosító szoftver futott. A virtualizációt biztosító szoftver beállítástól függően képes biztosítani, hogy a fizikai gépen futó egyes virtuális gépek elérjék egymást akár valós, akár belső, virtuális hálózaton keresztül. A virtualizációs szoftver lehet host alapú, amikor a virtualizációt megvalósító program csak egy az operációs rendszer által futtatott progamok között (1. ábra), illetve lehet hypervisor alapú, amikor a

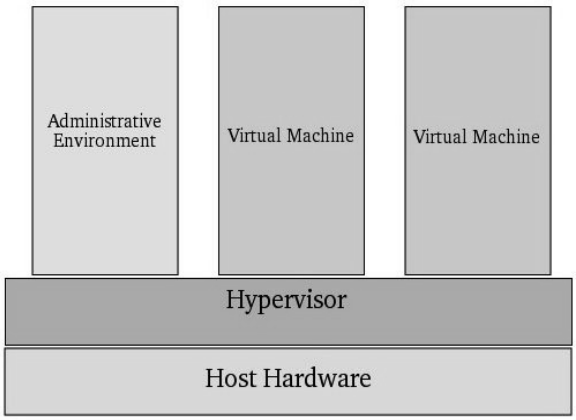
* *egyetemi tanársegéd, Miskolci Egyetem, IIT*
** *egyetemi tanár, Miskolci Egyetem, AIT*



1. ábra Hypervisor alapú virtualizáció

virtualizációt biztosító program közvetlenül a hardveren fut, operációs rendszertől függetlenül (2. ábra).

Host alapú például a VMWare-nek a Workstation elnevezésű terméke, vagy a Microsoft-nak a Virtual PC-je. Hypervisor alapú a VMWare-nek az ESX terméke, illetve a Microsoft-nak a Hyper-V szervere.



2. ábra Hypervisor alapú virtualizáció

A virtualizációt biztosító szoftver képes olyan virtuális gép emulálására, amely a valós géptől független: több-kevesebb memória, más grafikus kártya, más hangkártya, eltérő processzor.

Egy virtuális gépre telepített szerver funkciót biztosító szoftver lehet például egy file server (adattárolási szolgáltatással). Az a cég, amelyik ezt az adattárolást a saját gépparkján esetleg virtualizációval oldja meg, ilyen esetekben is tudja, hogy fizikailag hol tárolódnak az adatai. Az alkalmazott mentési stratégiának megfelelően például rendszeres időközönként archiválást végez a fizikai diszkről.

3. FELHŐK (CLOUD COMPUTING)

Létezhet azonban olyan eset, hogy egy felhasználó ezt a tárolási kapacítást bérli egy olyan személytől (vagy cégtől), aki a tárolást úgy oldja meg, hogy megadja ugyan a tárolási szolgáltatás elérhetőségét, de az adatok tárolását több tárolóhely között saját maga végzi. Ezek a tároló helyek között lehetnek valós és virtuális gépek is vegyesen. A biztonság érdekében a tárolás akár redundáns is lehet. Ebben az esetben az, aki a tárolási szolgáltatást igénybe veszi, nem tudja, hogy adatai a világon hol tárolódnak. Valójában (ha csak valami ok miatt nem szükséges ezt tudnia), akkor ez számára nem is fontos. Ilyen jellegű szolgáltatások esetében felhőkről (felhő alapú szolgáltatásokról) beszélünk. Bár a későbbiekben a felhő alapú szolgáltatások részletezésre kerülnek, érdemes elgondolkodni egyrészt azon, ez mit is jelent, másrészt pedig azon, miért lehet erre bárkinek is szüksége.

Az a felhasználó (fogyasztó) aki a szolgáltatást igénybe veszi tárolási szolgáltatás esetén saját személyes (céges) adatainak tárolását bízza rá egy idegen (akár konkurrens) cégre. Ez a cég a nála tárolt adatokat képes lehet olvasni, akár módosítani is. Ugyanakkor működési problémák is előfordulhatnak, és a tárolt adatok megsérülhetnek. Ki, milyen mértékben felelős? Kinek kell adatmentésről gondoskodni?

A másik kérdésre, hogy mi indokolhatja az ilyen jellegű szolgáltatások használatát, már könnyebb a válasz. Több olyan cég is létezik, ahol bizonyos időszak(ok)ban megnövelt hardver teljesítményre van szükség. Ilyen lehet például egy adóbevallás, amikor rövid idő alatt igen nagy sávszélességre, sűrű mentésre lehet igénye a megfelelő hatóságoknak. Ennek érdekében saját informatikai eszközparkjukat úgy kell méretezniük, hogy azok képesek legyenek ennek az időszaknak a megnövekedett igényét kiszolgálni. Az időszak leteltével azonban erre a teljesítményre már nincs szükségük egy évig. Az informatikai eszközöket beszerzés után rövid idővel később eladni általában nem kifizetődő. Az eszközök tehát kihasználatlanok lesznek. Ha azonban ezt határozott időszakra, szolgáltatásként igénylik, akkor a bevallási időszak elteltével egyszerűen csökkent mértékű szolgáltatást kell csak igényelniük.

Látható, hogy valóban van létjogosultságuk az ilyen számítási felhő alapú szolgáltatásoknak, de a biztonság speciális kérdéseket vet fel.

3. FELHŐ ALAPÚ SZOLGÁLTATÁSOK

Összefoglalva tehát: vannak szolgáltatók, akik az általuk biztosított szolgáltatás kivitelezését több számítógép segítségével úgy oldják meg, hogy az azt igénybe vevő felhasználó eléri ugyan a szolgáltatást, de nem tudja, hogy a szolgáltatást biztosító számítógép(ek)

a világban hol is van(nak).A felhő alapú szolgáltatások rövidítve xaaS-ként (x as a Service) adhatók meg.

3.1 SaaS (Software as a Service)

Az egyik legelterjedtebb szolgáltatás a szoftverek felhő alapú szolgáltatása. Ha nem is ilyen néven, de maga a fogalom korábban is létezett. A szoftverek license szerződése a legtöbb esetben külön kitér arra, hogy a szoftver vásárlója a vásárlással nem tulajdonjogot szerez a szoftver felett, hanem csak annak használhatóságáért fizet a vevő. Létezik több olyan konstrukció is, ahol rendszeres időközönként (például évente) újra és újra fizetni kell a szoftverért, a szoftver használatáért (tipikusan ilyenek a virusölő, vírus kereső szoftverek). Sokan nem rendelkeznek az általában a scanner-ekhez ingyenesen adott szövegfelismerő szoftverrel. Erre alapozva több olyan (ingyenes illetve fizetős) szolgáltatás érhető el az Interneten, amelyet úgy lehet igénybe venni, hogy fel kell tölteni azt a kép file-t, vagy pdf állományt, amelyre szöveg file-ként van szükség, majd a feldolgozott eredmény file letölthető szintén az Interneten keresztül. Vagy a jobb minőségű szolgáltatásért, vagy ha nagyobb méretű a file, általában fizetni kell.

Hasonlóan szolgáltatásként érhető el a Microsoft Office 365 nevű terméke: (http://www.microsoft.com/hu-hu/office365/online-software.aspx), illetve a Google cég Google Docs szoftvere (https://docs.google.com). Jellemző, hogy mivel a szoftver a szolgáltatónál fut, csak annyit tud, amire megírták. Amig a szolgáltató nem bővíti a szoftver lehetőségeit, addig ez nem is változik. Fizetni a szoftverért a felhasználás mértékének megfelelően kell. Ugyancsak jellemő, hogy az ilyen szoftverek nem veszik figyelembe a felhasználó egyedi igényeit. Nem egyedi megrendelésre készülnek, cél minél több példányban eladni. [2]

3.2 PaaS (Platform as a Service)

Sok esetben a felhasználó rendelkezik valamilyen szoftverrel, de nem rendelkezik megfelelő informatikai eszközzel, és azt működtető operációs rendszerrel. Szolgáltatásként azonban igénybe vehet ilyet. A legegyszerűbb ezt úgy elképzelni, hogy a felhasználó megkapja egy megfelelően specifikált virtuális gép elérhetőségét, amire az igényének megfelelő operációs rendszer már telepítve van. Erre felinstallálja saját szoftverét, és használja azt, majd fizet érte. Előnye a szolgáltatásnak, hogy nincs valódi beruházás, az operációs rendszert nem kell megvásárolnia, gyakorlatilag bérli az egész rendszert. Nem kell szerverszobát kiépíteni, klimatizálást megvalósítani. Nincsenek fenntartási költségek [2].

3.3 IaaS (Infrastructure as a Service)

Ez annyiban különbözik a PaaS-től, hogy nincs operációs rendszer, csak magát az infrastruktúrát veszi igénybe felhasználó, és azért fizet [2]. Fontos, hogy ebben az esetben (is) pontosan meg kell adnia, mit kell tudnia a hardvernek (memória méret, hálózati sebesség, tárolási és számítási kapacítás, stb.). A felhasználó valójában nem fogja tudni azt, hogy a szolgáltató ezt milyen módon biztosítja neki. Elképzelhető hogy több virtuális gép segítségével áll össze az igényelt teljesítmény. A biztosított gép rendszerfelügyelete, üzemeltetése már a felhasználó feladata.

4. BIZTONSÁGI KÉRDÉSEK

Felhő alapú szolgáltatások esetében fontos, hogy az igényelt szolgáltatás használatakor keletkező eredményhez ki férhet hozzá. Az eredmény ebben az esetben nem feltétlenül számítási eredmény, file tárolás esetében „eredmény” a feltöltött file. Három jellegzetes esetet szokás elkülöníteni:

- magán felhő (private cloud)
- közösségi felhő (Community cloud)
- nyilvános felhő (public cloud)

Magán felhő esetében szolgáltatást csak egy felhasználó érheti el. Erről a szolgáltatónak kell gondoskodnia. A biztosított szolgáltatás mások számára nem szabad, hogy hozzáférhető legyen. Sok esetben ezt a cég tűzfalán belül oldják meg a biztonság érdekében. Itt lehet a legkevésbé a költségeket megosztani, ezért a felhasználó számára általában ez a megoldás a legköltségesebb. A tűzfal azonban többnyire védelmet nyújt a kívülről érkező támadások ellen.

Közösségi felhő esetében azonos feladatot ellátó felhasználók esetében szokás beszélni. Például egyetemi felvételi esetében a felvételizőkről információkat itt helyezhet el a központi szervezet. A felhasználóknál levő alkalmazásoknak illeszkedniük kell ehhez a megoldáshoz, és komoly problémát okozhat, ha az egyes felhasználók mások adataihoz (is) hozzáférnek (kiderül, ki hova felvételizik még).

Nyilvános felhő esetében többen is hozzáférhetnek a szolgáltatáshoz. A szolgáltató feladata annak biztosítása, hogy az egyes felhasználók adatai ne keveredjenek össze, illetve mindenki csak a saját adataihoz férhessen hozzá. Komoly problémát okozhatna, ha például egy szövegfelismerésre feltöltött képfile esetében nem a saját felismert szöveg érkezne vissza, hanem egy másik cég szerződés tervezete, annak minden bizalmas adatával.

Ilyen nyilvános felhőre épül több elterjedt, részben ingyenes tárolási szolgáltatás: a Microsoft Skydrive-ja,

Google Drive-ja, vagy a szintén sokak által használt Dropbox, illetve SugarSync. Mindegyik szolgáltató esetében kritikus, hogy mennyire megbízható az adatok bizalmas kezelése.

Általában leszögezhető, hogy valódi biztonságot nem az egyedi megoldások jelentenek, hanem a szabványos biztonsági megoldások helyes alkalmazása. Olyan szolgáltatót érdmes választani, amelyik garantálja az adatok bizlmas kezelését, és azt, hogy az adatok nem lesznek jogosulatlanul hozzáférhetők.

Javasolt a felhő alapú szolgáltatások lépésenkénti bevezetése. Először olyan felhő alapú szolgáltatásokra érdemes áttérni, ahol a legkevesebb biztonsági probléma merülhet fel (például nincsnek szigorú törvényi kötelezettségek, mint a személyes adatok kezelése esetében).

A szolgáltatások jellemzően egy előzetes szerződés kötés után lesznek elérhetők, A szerződésnek célszerű arra kitérnie, hogy egyes problémás bekövetkezése esetén (például adatvesztés) ki milyen mértékben felelős, valamint arra, hogy a szolgáltatás használatához kinek milyen módon kell hozzájárulnia (kinek a feladata például egy PaaS esetén a rendszeres archiválás).

A szolgáltatást biztosító számítógépeket természetesen érhetik a szokásos, elterjedt támadások:

- a DoS támadás (a szolgáltatás lassítása, leállítása),
- a spoofing (lehallgatással történő információ szerzés),
- a hálózati forgalom meghamisítása,
- a megszemélyesítés, stb.

Ezek ellen a szolgáltatónak megfelelő módon védekeznie kell, illetve a szerződésnek megdelelően segítséget nyújtania a felhasználó számára, hogy abból az irányból a szolgáltatás lehetőleg ne legyen támadható.

5. ÖSSZEGZÉS

A felhő alapú szolgáltatások előnyösek mind a szolgáltatást biztosítók, mind az azt igénybevevők számára. A számítási felhők elterjedése egyre gyorsabb. Ennek köszönhetően várhatóan egyre szélesebb körben fogják a szolgáltatást biztosító eszközparkot illetve a felhasználók eszközeit támadni. A támadás célja vagy információ szerzés, vagy az információk megváltoztatása, törlése. A felhasználók egyik legfontosabb feladata a szolgáltatást biztosító cégek megfelelő kiválasztása, helyes szolgáltató szerződés kötése, megfelelő biztonsági szabályzat kialakítása, betartása. [3]

6. KÖSZÖNETNYILVÁNÍTÁS

A bemutatott kutató munka a TÁMOP-4.2.1.B-10/2/KONV-2010-0001 jelű projekt részeként az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

7. IRODALOM

[1.] http://hu.wikipedia.org/wiki/Moore-törvény
[2.] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
(A NIST Definition of Cloud Computing)
[3.] http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
(Guidelines on Security and Privacy in Public Cloud Computing)