CTI Jelentés

A felhőtárhely-szolgáltatások kiberbiztonsági kérdései a szolgáltató szempontjából

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék

Bevezetés

Legyen szó felhőbiztonsági szolgáltatások telepítéséről a rendszerek és az adatok jobb védelme érdekében, vagy felhőbeli számítási feladatok használatáról a hozzáférhetőség, a skálázhatóság, vagy az alkalmazottak és partnerek közötti kommunikáció és együttműködés javítása érdekében, a felhő napjaink digitális átalakulásának szerves részét képezi.

A felhőszolgáltatás a vállalatok és az ügyfelek számára az interneten keresztül igény szerint nyújtott szolgáltatások széles körére utal. Ezeket a szolgáltatásokat úgy tervezték, hogy belső infrastruktúra vagy hardver nélkül, egyszerűen és megfizethető áron biztosítsanak hozzáférést az alkalmazásokhoz és erőforrásokhoz.

A felhőalapú számítástechnika és az ezeket a szolgáltatásokat nyújtó 10 legnagyobb felhőszolgáltató (Amazon Web Services (AWS), a Microsoft Azure, a Google Cloud Platform (GCP), az Alibaba Cloud, az Oracle Cloud, az IBM Cloud (Kyndryl), a Tencent Cloud, az OVHcloud, a DigitalOcean és a Linode) alapvető változásokat hozott az informatikai infrastruktúra piaci hátterében világszerte. Ebben az útmutatóban ismertetve lesz a felhőkörnyezet biztosításának kihívásai és az, hogy mikre kell figyelni egy felhőkörnyezet kialakításakor.

A felhőszolgáltatások olyan technológiákon alapulnak, amelyek lehetővé teszik a felhasználó számára, hogy igény szerint virtuális kiszolgálókat és számítási erőforrásokat építsenek ki. A kiugró használat és forgalom hatására redundanciát valósítson meg a magas rendelkezésre állás érdekében.

A virtualizáció egy olyan technológia, ami lehetővé teszi a hardverek maximális kihasználását. Lehetségessé válik a hardverek hatékony megosztása több felhasználó és alkalmazás között, és lehetővé teszi a felhő méretezhetőségét, agilitását és rugalmasságát. A virtualizáció egy virtuális operációs rendszer, szerver, tárolóeszköz vagy hálózati erőforrás létrehozásának folyamata. Virtuális gépek létrehozása és a konténerizáció is alkalmas a rugalmasság növelésére, az erőforrásigény minimálisra csökkentésére és a funkciók maximalizálására. A virtuális gépek olyan számítógépes programok, amelyek tényleges számítógépként viselkednek. A konténerek pedig egy virtuális gépnek megfelelő fájlegyüttes, amely tartalmaz minden olyan kiegészítést, ami szükséges az igényelt futtatott programhoz. A virtuális gépeknek szükségük van egy külső hálózati kártyára (ami lehetővé teszi a hálózathoz történő csatlakozást), vagy VLAN-ra (virtuális helyi hálózatra, aminek tagjai úgy kommunikálnak, mintha ugyanabba a helyi hálózatba tartoznának, fizikai elhelyezkedésüktől függetlenül).

Egy felügyeleti szoftver központosított irányítást biztosít a rendszergazdáknak az infrastruktúra és a rajta futó alkalmazások felett.

Az automatizálás felgyorsítja azokat a feladatokat, amelyeket manuálisan és ismételten lenne szükséges végrehajtani. Az automatizálás csökkenti az emberi beavatkozás szükségességét, a hibalehetőséget és a költségeket.

Felhőszolgáltatások üzembe helyezési modellek

A felhőtárhely struktúráknak három főbb típusa van a hozzáférhetőség szerint: nyilvános, privát és hibrid felhő. A felhőalapú rendszerek mindegyik típusának megvannak az előnyei és jó eséllyel nem mindenkinek felelnek meg kivétel nélkül, ezért nagyon fontos, hogy specifikálva legyen az, hogy mire is van konkrétan szüksége az ügyfélnek.

Nyilvános felhő

A nyilvános felhő a felhőszolgáltatások leggyakoribb típusa. Itt a számítási erőforrásokat olyan külső szolgáltatók biztosítják, mint például az Amazon, a Google vagy a Microsoft. Az eszközállomány teljes egésze (tárhely, hálózat, számítási kapacitás) a szolgáltató tulajdonában van és ő is látja el az üzemeltetési feladatokat. A nyilvános felhőtárhely esetében több felhasználónak van hozzáférése ugyanahhoz a felhőhöz, ezért rendkívül fontos az ügyfelek teljes szeparációja. A biztonsági feladatokat és megoldásokat szintúgy a szolgáltató látja el.

A felhasználó feladata abban merül ki, hogy az adatait kellő óvatossággal kezelje és megfeleljen a szolgáltató általi előírásoknak. Amennyiben harmadik féltől származó programot szeretne használni a felhőkörnyezetben, annak biztonságossá tétele is a felhasználó feladata.

A végzett tevékenységeket naplózni kell az auditálás miatt, bár ez kisebb cégekre nem jellemző.

A nyilvános felhő könnyen kezelhető, hozzáférhető, megosztható, illetve könnyen változtatható a kapacitása. A hátránya, hogy a felhasználónak viszonylag kevés, vagy semmilyen kontrollja sincsen afelől, hogy az adatok hol tárolódnak, azonban például a különféle jogszabályok miatt a régió opcionálisan megválasztható.

Előnyei közé tartozik, hogy lényegesen kisebb költség terheli a felhasználót (csak a szolgáltatásért fizet, minden feladatot a szolgáltató lát el), nagyfokú skálázhatósági lehetőségeket biztosít és nagy a megbízhatósági szintje.

Privát felhő

Egy privát felhő olyan erőforrások összesége, amely kizárólag egyetlen ügyfél számára vannak kialakítva. Fizikailag elhelyezhető az ügyfél adatközpontjában vagy külső felhőszolgáltatónál is, azonban a szolgáltatások mindig magánhálózaton keresztül biztosítottak. A privát felhőt legtöbbször olyan szervezetek és intézmények veszik igénybe (állami-, banki szféra stb.), akik számára kritikus fontosságú a tevékenységeikhez a magasfokú ellenőrzési és felügyeleti részvétel.

A privát felhő könnyebb módot biztosít a szabályozásra, valamint az üzemeltetőknek nagyobb rálátást ad a biztonságra és a hozzáférések szabályozására például saját tűzfalszabályok létrehozásával. A szabályozási előírásoknak megfelelően nem szükséges a szolgáltatóra támaszkodni. A privát felhő velejárója, hogy lényegesen magasabb költségek terhelhetik a vállalatot, mivel minden változtatást (pl. skálázás) önmagának kell megoldania és finanszíroznia.

A privát felhő előnyei, hogy a hardver és szoftverállományt egyénileg alakíthatja ki annak tulajdonosa. A felhasználók számára a biztonság növelése érdekében a hozzáférések, a jogosultsági szinteknek megfelelően kerülnek kiválasztásra.

Hibrid felhő

A hibrid felhő olyan számítástechnikai környezet, amely egy helyszíni adatközpontot egyesít egy nyilvános felhővel, így lehetővé téve az adatok és alkalmazások megosztását közöttük.

Erre akkor van szükség, ha a számítási és feldolgozási igény meghaladja a helyszíni adatközpont képességeit. A vállalkozás a felhő segítségével azonnal fel-, vagy leskálázhatja a kapacitást, így el tudja kerülni új szerverek vásárlásának, telepítésének és karbantartásának idejét és költségeit, amelyekre nem mindig van szüksége.

A környezet eredménye egy egyénre szabott, átfogó infrastruktúra, ami lehetővé teszi a vállalkozás számára, hogy jobb megközelítést alkalmazzon informatikájában. A szolgáltatók, platformok és szoftverszolgáltatásopciók optimális kombinációját alkalmazva elkerülhetővé válik ezzel a gyártóktól való függés. Lehetővé válik a gyors reagálás és a versenyképesség megőrzése úgy, hogy a terheléseken igény szerint változtathat.

Felhőszolgáltatási modellek

A felhőalapú számítási szolgáltatások típusai olyan szolgáltatás-üzembehelyezési modellek, amelyek eltérő mértékű szabályozást tesznek lehetővé az információt és a nyújtott szolgáltatások típusait illetően. A felhőalapú számítási szolgáltatások fő típusai az alábbiak.

Szolgáltatásként nyújtott infrastruktúra

Az első az Infrastructure-as-a-Service (IaaS) vagyis a szolgáltatásként nyújtott infrastruktúra. Itt számítás, tárolás és hálózatkezelés történik havidíjért cserébe. Ugyanazokat a funkciókat nyújtja, mint a hagyományos infrastruktúra, anélkül, hogy fizikailag be kellene állítani és karban kellene tartani. Ehelyett csak a használat alapján fizetendő a bérlés.

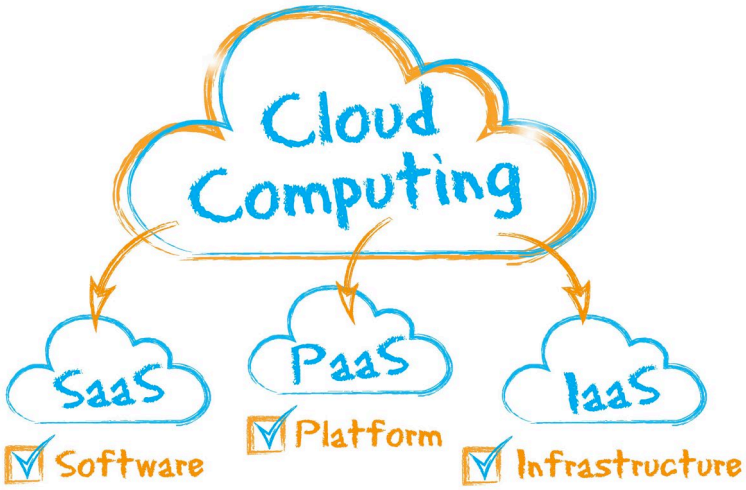
Szolgáltatásként nyújtott platform

A másik a Platform-as-a-Service (PaaS), azaz szolgáltatásként nyújtott platform. Ezzel a szolgáltatással az előzőeken túl még közbenső szoftvereket, fejlesztőeszközöket, üzleti intelligencia szolgáltatásokat, adatbáziskezelő rendszereket és még sok minden mást is lehet használni. A PaaS a teljes webalkalmazás fejlesztési életciklust (fejlesztés, tesztelés, üzembe helyezés, felügyelet és frissítés) támogatja.

Szolgáltatásként nyújtott szoftver

A harmadik a Software-as-a-service (SaaS), azaz szolgáltatásként nyújtott szoftver. Lehetővé teszi, hogy az interneten keresztül felhőalapú applikációkhoz kapcsolódjon és használja azokat.

A háttér-infrastruktúra, a közbenső szoftverek, az applikáció és az applikációadatok teljes egészében a felhőszolgáltató adatközpontjában találhatók. A felhőszolgáltató felügyeli a hardvereszközöket, valamint a szoftvert, és a megfelelő szolgáltatási szerződés alapján gondoskodik az applikáció és az adatok elérhetőségéről és biztonságáról is.



Kiszolgáló nélküli modell

A kiszolgáló nélküli számítástechnika használatával a fejlesztők gyorsabban fejleszthetnek alkalmazásokat, mivel nincs szükség arra, hogy ők kezeljék az infrastruktúrát. A kiszolgáló nélküli alkalmazások esetében a felhőszolgáltató automatikusan kiépíti, skálázza és kezeli a kód futtatásához szükséges infrastruktúrát.

A modell megértéséhez fontos azt is tudni, hogy továbbra is kiszolgálók futtatják a kódot. A „kiszolgáló nélküli" kifejezés arra utal, hogy az infrastruktúra kiépítésével és kezelésével kapcsolatos feladatok a fejlesztő számára láthatatlanok. Ez a megközelítés lehetővé teszi a fejlesztők számára, hogy az üzleti logikára koncentráljanak, és így több üzleti szempontból lényeges értéket hozzanak létre.

Felhőszolgáltató felelősségei

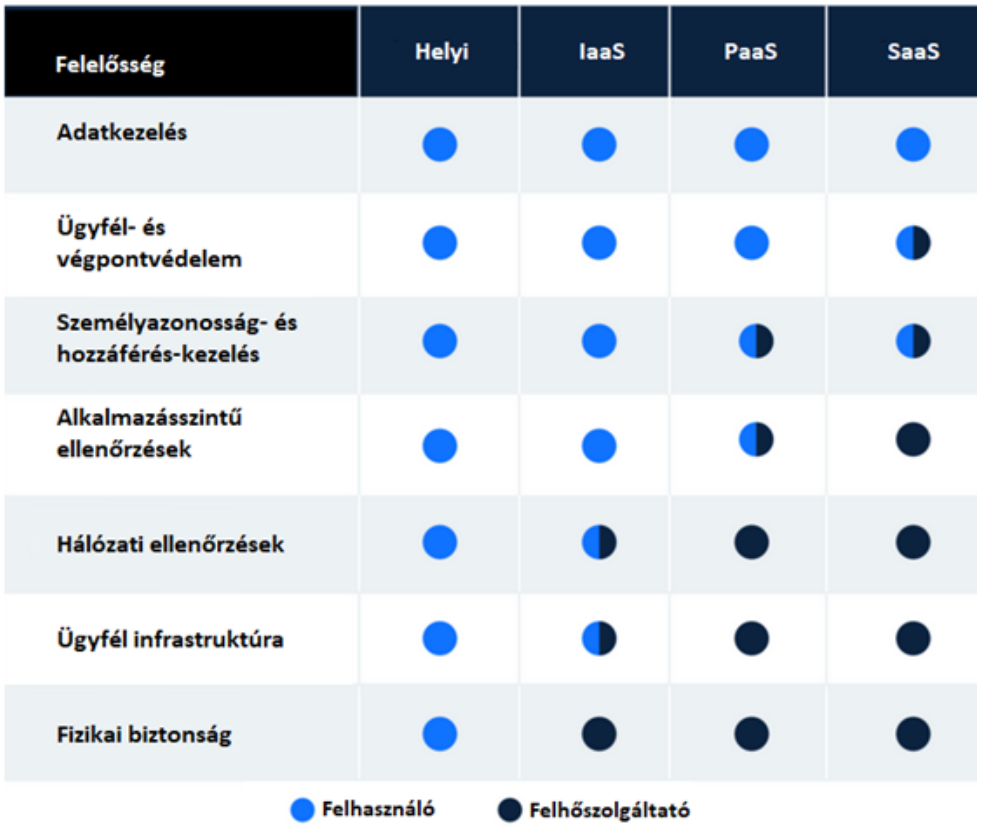
A nyilvános felhőalapú számítástechnikát fontolgató szervezetek tévesen azt feltételezik, hogy a felhőbe való átköltözés után az adatok védelmében betöltött szerepük teljes mértékben a felhőszolgáltatóra hárul.

A megosztott felelősség modell

Egyszerűen fogalmazva ez annyit jelent, hogy a felhőszolgáltató felel a felhő fizikai biztonságáért, míg az ügyfél a felhőbeni biztonságért.

Lényegében a felhőszolgáltató felelős azért, hogy a platformján belül felépített infrastruktúra eredendően biztonságos és megbízható legyen. A biztonságos felhő működtetése érdekében a felhőszolgáltató kezeli és ellenőrzi a hoszt operációs rendszert és a virtualizációs réteget. Ők garantálják a létesítmények fizikai biztonságát is.

A felhasználói oldalon a testreszabható felhőfunkciók, például az alkalmazáskezelés, a hálózati konfiguráció és a titkosítás az ügyfél felelőssége. Az adott felhőkörnyezeten belüli biztonság garantálása érdekében az ügyfél konfigurálja és kezeli a vendég operációs rendszer és más alkalmazások biztonsági ellenőrzését (beleértve a frissítéseket és a biztonsági javításokat), valamint a biztonsági csoport tűzfalát.



Megosztott felelősség modell

DDoS elleni védelem

A DDoS (Distributed Denial of Service) támadásnak azt nevezik, amikor a támadó nagy mennyiségű forgalommal áraszt el egy hálózatot vagy szervert azzal a céllal, hogy annak működését ellehetetlenítse. Ilyenkor a szolgáltatások ideiglenesen vagy hosszú távon nem elérhetőek. A témával kapcsolatban bővebb információk olvashatók az NBSZ NKI kegy korábbi segédletében.

Hálózati redundancia

A hálózati redundancia egy olyan kommunikációs útvonal, amely további linkekkel rendelkezik az összes csomópont összekapcsolására, ha az egyik link kiesik. Vagyis a különböző kommunikációs kapcsolatok vagy eszközök meghibásodása esetén a redundancia teszi lehetővé, hogy a hálózat, a kiszolgálók és az internetkapcsolat továbbra is üzemben maradjon, alternatív kommunikációs útvonalak és tartalékberendezések biztosításával. A felhőszolgáltatók törekednek a közel 100%-os üzemidőre, de ennek ellenére is történhetnek kimaradások.

Fizikai redundancia

A hardver redundancia egy hardver összetevő, két vagy több fizikai példány biztosításával érhető el, több tápegység, hálózati kártya és hűtőventilátor használatával.

RAID

Az adatok biztonságos tárolásához segítséget nyújt a RAID (Redundant Array of Independent Drives vagy Redundant Array of Inexpensive Disks) technológia. Ez egy olyan tárolási megoldás, amely több lemezmeghajtót egyesít egyetlen egységbe. Előnyei a magas rendelkezésre állás és a jobb teljesítmény. A RAID funkciókat ellátó és a meghajtókat vezérlő szoftver egy külön vezérlőkártyán (hardveres RAID vezérlő), vagy egyszerűen egy illesztőprogramban található. A RAID alapötlete a lemezegységek csíkokra (stripes) bontása, azonban ezek nem azonosak a lemez fizikai sávjaival (tracks), amit az angol és magyar elnevezés különbözősége is jelez.

RAID 1

A RAID 1 eljárás alapja az adatok tükrözése (disk mirroring), azaz az információk egyidejű tárolása a tömb minden elemén. RAID 1 tömb létrehozásához legalább két meghajtóra van szükség. Ha egy meghajtó meghibásodik, akkor a másik meghajtót használja az adatok helyreállításához és a folyamatos működéshez. Hátránya, hogy a tényleges tárolókapacitás a teljes meghajtókapacitásnak a fele, mivel minden adat kétszer íródik.

RAID 5

A leggyakrabban használt RAID szint, ami legalább 3 meghajtót igényel, de akár 16-tal is lehet használni. Az adatblokk fel van bontva a meghajtók között és a paritásadatok nem rögzített meghajtóra vannak írva, hanem az összes meghajtón eloszlanak. A paritásadatok felhasználásával a hibás meghajtó adatait a vezérlő a többi meghajtóról ki tudja számolni. Ez azt jelenti, hogy a RAID 5 egyetlen meghajtó meghibásodását is kibírja anélkül, hogy elveszítené az adatokat vagy az adatokhoz való hozzáférést. Bár a RAID 5 szoftveresen is elérhető, hardvervezérlő használata ajánlott. Ezeken a vezérlőkön gyakran extra gyorsítótárat-memóriát használnak az írási teljesítmény javítása érdekében.

RAID 6

A RAID 6 a RAID 5 kiterjesztése, ahol ugyan a paritásinformációk dupla akkora helyet foglalnak és egyel több tárolóra is szükség van, cserébe viszont két meghajtó kiesését is elviseli a rendszer.

További RAID módok

A fentieken kívül létezik még a RAID 0, ahol a fájlok tartalmát egyenletesen elosztja a merevlemezek között. Ennek a konstrukciónak nem a redundancia a lényege, hanem a nagy sebesség elérése.

A RAID 0+1 megoldás ötvözi a RAID 0 gyorsaságát a RAID 1 megbízhatóságával, azonban ez költséges és a helykihasználása sem megfelelő.

A RAID 10 a RAID 0+1 fordítottja. Biztonságot nyújt azáltal, hogy tükrözi az összes adatot a másodlagos meghajtókon, miközben csíkozást használ az egyes meghajtók között az adatátvitel felgyorsítása érdekében. Komoly hátránya, hogy a tárolókapacitás fele tükrözésre megy. A RAID 5 vagy RAID 6 tömbökhöz képest drágább módja a redundanciának.

A teljes biztonság érdekében továbbra is ajánlott biztonsági másolat készítése a RAID rendszeren tárolt adatokról.

Titkosítás

Az adatok titkosítása védelmet nyújt a jogosulatlan hozzáféréssel szemben. A megfelelően implementált titkosítási szabályzat további rétegeket biztosít a felhőalapú számítási feladatok számára. Emellett védelmet nyújt a támadók és más jogosulatlan felhasználók ellen mind a szervezeten belül, mind a hálózaton kívülről.

Adattitkosítási módszerek

Szimmetrikus titkosítás: Szimmetrikus titkosítás esetén a rendszer ugyanazt a kulcsot használja a titkosítás és a visszafejtés végrehajtásához is. A kulcs másolatának birtokában lévő személy visszafejtheti és titkosíthatja az információkat.

Aszimmetrikus titkosítás: Az aszimmetrikus titkosítási folyamat két kulcsot tartalmaz: egy nyilvános kulcsot és egy privát kulcsot. Bárki, aki rendelkezik a nyilvános kulccsal, könnyen küldhet információkat biztonságosan és azt csak a privát kulccsal rendelkezők tudják visszafejteni.

Kulcskezelés

Az adatok felhőbeli titkosítása a titkosítási kulcsok biztonságos tárolásától, felügyeletétől és működési használatától függ. A **kulcskezelő rendszer kritikus fontosságú** a szervezet titkosítási kulcsok létrehozására, tárolására és kezelésére való képességében. A kulcskezelő rendszer a fontos jelszavakat, kapcsolati stringeket és egyéb bizalmas informatikai információkat is titkosítja.

Ezek a kezelők az adatokat átvitel során TLS-sel (Transport Layer Security) és AES-256 bites (Advanced Encryption Standard) titkosítási kulccsal titkosítják. A TLS kritikus szerepet játszik az interneten keresztüli adatátvitel biztonságossá tételében, és az AES-256 szerves része a legbiztonságosabb konfigurációiknak. Az AES az egyik legnépszerűbb szimmetrikus kulcsú titkosítási algoritmus.

A felhőszolgáltatók titkosítási szolgáltatásai közé tartozik a Google Secret Manager, az Azure Key Vault és az AWS Key Management Service.

A leggyakrabban használt titkosítás típusai:

- **Titkosítás átvitel közben (in-transit):** Megvédi a továbbítás során az adatokat és üzeneteket. Amikor letöltésre kerül valami a felhőből, ez megvédi az adatokat, miközben azok a felhőből az eszközre kerülnek.
- **Titkosítás inaktív állapotban(at-rest):** Ez a fajta titkosítás megvédi az adatokat vagy a fájljokat a szerveren, amíg nincs használatban. A fájlok így védve maradnak, amíg tárolják őket.

A legtöbb nagy szolgáltató biztosítja azt a funkciót, amely nemcsak a felhőalapú tárolást és az adatokat, hanem a felhőkörnyezetben lévő virtuális gépeket is titkosítja.

Zero-knowledge proof

A Zero-knowledge a privát, végponttól végpontig tartó titkosítás alternatív neve. A privát azt jelenti, hogy a felhasználón kívül senki más nem olvashatja a fájlokat. Ez azért van így, mert a titkosítás a helyi eszközön történik, mielőtt a fájlok átkerülnének a felhőbe. A "végponttól végpontig" arra utal, hogy olyan jelszót használ, amelyet csak a felhasználó ismer, vagyis az átvitel után senki sem tudja visszafejteni a fájlokat.

Egy zéró tudású szolgáltatás nem tudja a titkosítatlan adatot egy kormánynak vagy egy célzott marketingügynökségnek átadni. Amennyiben a felhasználó elfelejti a jelszavát, a szolgáltatás nem visszaállítható. Ennek elkerülése érdekében egy jelszómenedzser használata javasolt a jelszavak tárolására.

Terheléselosztás

A terheléselosztás egy olyan módszer, amellyel feladatokat lehet szétosztani számítógép klasztereken (csoportokon), hálózati kapcsolatokon, processzorokon, merevlemezeken. Ennek a célja, hogy az ügyfelek és a szervezetek számára hatékonyabbak és elérhetőbbek legyenek a munkafolyamatok és a szolgáltatások. A felhőbeli terheléselosztás magában foglalja a hálózati forgalom és a szolgáltatások folyamatos fenntartását.

Az internetes forgalom napról napra növekszik, ami a szerverek túlterheléséhez vezethet, főleg a népszerű webszerverek esetében. Két alapvető megoldás létezik a szerverek túlterheltségének leküzdésére:

- Az egykiszolgálós megoldás az, amikor a meglévő szervert egy nagyobb teljesítményű szerverre cserélik. A módszer nem mindig célravezető, mert az új szerver hamarosan ismét túlterhelt lehet, ami újabb frissítést igényel. Ezenkívül a korszerűsítési folyamat fáradtságos és költséges.

- A többszerveres megoldás az, amelyben van egy skálázható szolgáltatási rendszer egy szerver klaszterben. Ez költséghatékonyabb, valamint a szolgáltatások szempontjából jobban skálázható.

A terheléselosztást egy dedikált hardvereszköz vagy program biztosítja. A felhőalapú szerverfarmok pontosabb skálázhatóságot és rendelkezésre állást érhetnek el így.

A terheléselosztási megoldások két típusba sorolhatóak:

- Hardveralapú terheléselosztó: Olyan fizikai eszköz, amelyet a webes forgalom több szerver között történő elosztására használnak.

- Szoftveralapú terheléselosztó: Annyit jelent, hogy szabványos hardveren (asztali számítógépek) és szabványos operációs rendszereken futnak. Feladata ugyanaz, mint a hardveralapúnak, azonban lassabb annál.

Amikor egy terheléselosztóval rendelkező webhely kap egy kérést, a terheléselosztó fogadja először a kérést, majd továbbítja azt a mögötte lévő több szerver egyikére. A terheléselosztó különböző algoritmusokat használ annak eldöntésére, hogy melyik szerver a legalkalmasabb a kérés kezelésére. Az egyik ilyen algoritmus a round-robin, amely minden egyes szerverre sorban elküldi a kérést. A másik algoritmus a súlyozott, amely ellenőrzi, hogy egy szerver éppen hány kéréssel foglalkozik, és a legkevésbé terhelt szerverre küldi a kérést.

Ügyfelek elkülönítése

Az elkülönítési technikák biztosítják, hogy egy felhasználó szolgáltatása ne férhessen hozzá egy másik felhasználó szolgáltatásához (vagy adataihoz), illetve ne befolyásolhassa azt. A nagy felhőszolgáltatások számos különböző szolgáltatást kínálhatnak és ezek mindegyike más-más megközelítést alkalmazhat az adatok elkülönítésére.

Hálózati és tárolási virtualizációs technológiák segítségével jó szeparációt lehet elérni. Ezekkel akadályozzák meg, hogy illetéktelen felek hozzáférjenek a felhőszolgáltatásban tárolt adatokhoz.

A felhőszolgáltatások központi hozzáférés-szabályozási mechanizmust használnak annak meghatározására, hogy mely szolgáltatás- és felhasználói identitások férhetnek hozzá a tárolt objektumokhoz. A felhőszolgáltatás ügyfelei közötti biztonsági elválasztás csak akkor lesz hatékony, ha a szolgáltató hatékony sebezhetőségkezelési tervvel rendelkezik.

Operációs rendszerek, webkiszolgálók vagy más alkalmazások biztosítják a szolgáltatások és a felhasználók közötti szükséges elkülönítést. Ezzel a módszerrel azonban a szélhámos felhasználók számára elérhető támadási felület sokkal nagyobb. A szoftveres biztonsági rések vagy a helytelen konfigurációs problémák jogsértésekhez vezethetnek.

Összegzés

A nyilvános felhőszolgáltatók elősegítik az elosztott felhő-számítástechnika eredendő hatékonyságát, ami lehetővé teszi innovatív szoftveralkalmazások és platformok kiépítését, ugyanakkor javítja az információbiztonságot és az adatvédelmi ellenőrzéseket. Mint ilyen, kritikus fontosságú megérteni az egyes vezető felhőszolgáltatókat, valamint azok különböző stratégiáit.

Források

- https://www.geeksforgeeks.org/security-issues-in-cloud-computing/
- https://dgtlinfra.com/top-10-cloud-service-providers-2022/
- https://blog.real.com/how-to-set-up-a-personal-cloud/
- https://www.techtarget.com/searchsecurity/feature/The-importance-of-security-data-encryption-for-cloud
- https://www.techtarget.com/searchsecurity/tip/All-about-cloud-native-application-protection-platforms?_gl=1*3toac*_ga*MjA2NzEzMTgzMi4xNjY4MTU1NzE0*_gaTQKE4GS5P9*MTY2ODE1NTcxMy4xLjEuMTY2ODE1OTQ0MS4wLjAuMA..&_ga=2.31172413.306762570.1668155714-2067131832.1668155714
- https://www.quest-technology-group.com/academy/what-is-data-in-transit-vs-data-at-rest
- https://home.kpmg/ch/en/blogs/home/posts/2021/06/cloud-security-provider-responsibility.html
- https://www.aquasec.com/cloud-native-academy/cspm/cloud-infrastructure-security/
- https://reciprocity.com/blog/the-6-key-pillars-of-cloud-security/
- https://reciprocity.com/resources/what-is-cloud-cryptography-how-does-it-work/
- https://www.websiterating.com/cloud-storage/what-is-zero-knowledge-encryption/
- https://www.microsoft.com/hu-hu/security/business/security-101/what-is-cloud-security
- https://www.geeksforgeeks.org/load-balancing-in-cloud-computing/
- https://www.ncsc.gov.uk/collection/cloud
- https://www.ibm.com/topics/private-cloud
- https://cloudcheckr.com/cloud-security/shared-responsibility-model/
- https://www.cloudwards.net/cloud-security/
- https://www.serverwatch.com/guides/load-balancing-software/

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2023