Oláh István – Magyar Sándor

Biztonsági kérdések egy publikus felhőben

Military and Intelligence CyberSecurity Research Paper
2023/1.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

BEVEZETÉS[1]

Napjainkban a felhő technológiával kialakított informatikai szolgáltatások rohamosan terjednek. Ennek alapvető oka az egyre gyorsuló innovációból származó folyamatosan növekvő igény az informatikai erőforrásokra, az egyre komplexebb tudást igénylő rendszerek. Egy szerver kiszolgálót beszerezni, üzembe állítani, az üzemeltetési feladatokat kialakítani, a szakembereket kiképezni saját telephelyen több hetet, hónapot is – vagy akár ennél sokkal hosszabb időtartamot is – meghaladhatja. Ezzel szemben ugyanazt az erőforrást, üzemeltetéssel együtt jelentősen rövidebb idő alatt képes egy felhőszolgálató biztosítani. Egy szervezet belső folyamatainak működéséhez a felhőszolgáltató által nyújtott szolgálatatásoknak a szervezet szempontjából az informatikai rendszerekre meghatározott SLA[2]-i szerint szükséges rendelkezésre állni. Amennyiben egy szervezet igénybe vesz felhőszolgáltatást, akkor arra célszerű a rendelkezésre állási feltételeket is meghatározni, mert ezen informatikai elemek ugyanúgy részei a működési ökoszisztémának, a szolgáltatási és ellátási láncoknak. Ez a felfogás jelenik meg a 2023. januárban hatályba lépett CER-ben[3], NIS2[4]-ben, valamint a DORA[5] irányelvekben.

A FELHŐSZOLGÁLTATÁSOK FAJTÁI

A felhőszolgáltatások meghatározása jogszabályban nem szerepel. A gyakorlatban az NIST (National Institute of Standards and Technology) 800-145[6] számon publikált szakmai ajánlásban szereplő definíciókat alkalmazzák. A szolgáltatások közös jellemzői:

- a szolgáltatást az adott pillanatban a szükséges mértékig, esetenként önkiszolgálóan vehetik igénybe,
- alapvető a hálózat elérése,
- az erőforrások megosztott használata, az igénybe vevők közt,

[1] A mű a Katonai Nemzetbiztonsági Szolgálat TKP2021-NVA-24 azonosító számú „A mesterséges intelligencia alkalmazásának kutatása a katonai nemzetbiztonsági célú adatszerző, adatfeldolgozó és vizualizációs eljárásokban, és kapcsolódó fejlesztések elvégzése” elnevezésű projektje keretében, az Innovációs és Technológiai Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával valósult meg.

[2] Service Level Agreement (SLA) szolgáltatási szintre vonatkozó megállapodás.

[3] Az Európai Parlament és a Tanács (EU) 2022/2557 IRÁNYELVE a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről, 2022. december 14.

[4] Az Európai Parlament és a Tanács (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, 2022. december 14.

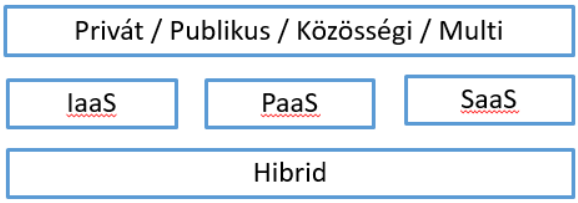
[5] Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete a pénzügyi ágazat digitális működési rezilienciájáról, 2022. december 14.

[6] Special Publication 800-145, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

– a szükséges működési kapacitások lekövetése, dinamikus erőforrássokkal és az igénybe vett szolgáltatásokkal arányos díj fizetése.

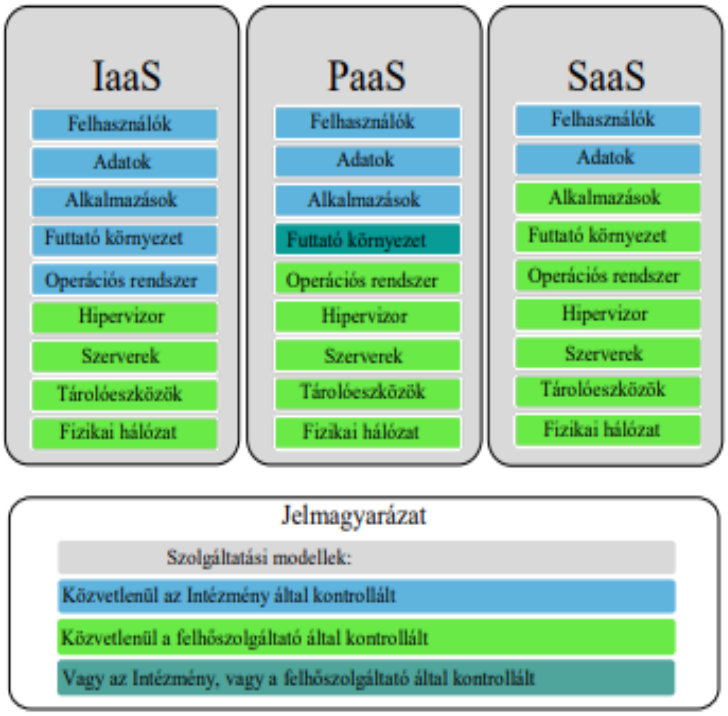
A Magyar Nemzeti Bank (MNB) 2019. április elsején adta ki ajánlását a közösségi és publikus felhőszolgálatatások igénybevételéről 4/2019. számon (a továbbiakban: MNB ajánlás).

Fiegyelembe véve a tulajdonjogot, az igénybe vett szolgáltatások jellegét, tartalmát, a földrajzi elhelyezkedést az alábbi esetek létezhetnek az NIST szerint:



1. ábra: A felhőszolgáltatások csoportosítása.
Forrás: a szerzők

A kockázatok kezelése szolgáltatási szempontjából a szolgálgató és az igénybe vevő közt a felelősséget az informatikai ökoszisztéma szinteken egyértelműen meg kell határozni. Az MNB ajánlása szerint:



2. ábra: Szolgáltatási modellek és az elemek feletti kontrollok közevetlen gyakorlói. [7]

[7] A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről

Fontos kiemelni, hogy a pénzügyi szektorban a felhasználók kezeléséért, az adatok bizalmasságáért az igénybevevő – pénzintézet – a felelős minden esetben az alábbi igénybe vett szolgáltatások szerint:

- IaaS (Infrastructure as a Service), amikor az alap infrastruktúrát vesszük igénybe;
- PaaS (Platform as a Service), amikor már operációs rendszer és/vagy futtatási környeztet is része a szolgáltatásnak;
- SaaS (Software as a Service), amikor a fentieken túl – az adatok és a felhasználók kiételével – mindent a szolgálató biztosít.

Az igénybe vett szolgáltatás bármi lehet ma már a gyakorlatban. Erre példa:

+ Address Verification as a Service
+ **Anything as a Service**
+ API as a service (APIaaS) Application
+ Delivery as a Service
+ Application Platform as a Service
+ Architecture as a Service
+ Authentication as a Service
+ Backend as a Service
+ Backup as a Service
+ Big Data as a Service
+ Broker as a Service
+ Business as a Service
+ Business Process as a Service
+ Cloud Load Balancers as a Service
+ Cloud Search as a Service
+ Collaboration-as-a-Service
+ Commerce as a Service
+ Communication as a Service
+ Computing as a Service
+ Contact Center as a Service
+ Conversations as a Service
+ Data as a service
+ Database as a service
+ Desktop as a Service
+ Development as a Service
+ DevTest as a Service
+ Disaster Recovery as a Service
+ Drupal as a Service
+ Email as a Service
+ Encryption as a Service
+ Enterprise Resource Management as a Service
+ Ethernet as a Service
+ **Everything as a Service**
+ Firewall as a Service
+ Framework as a Service
+ Globalization as a Service
+ Hadoop as a Service
+ Hardware as a Service
+ High Performance Computing as a Service
+ Identity as a Service
+ (Infrastructure PaaS)
+ Insight as a Service
+ Integrated Development Environment as a Service
+ Integration as a Service Integration Platform as a Service
+ Integration Platform as a Service
+ **IT as a Service**
+ Java Platform as a Service
+ Knowledge as a Service
+ Light as a Service
+ Logon as a Service Management as a Service
+ Mashups as a Service
+ Message Queuing as a Service
+ Metal as a Service
+ Mobility as a Service
+ Mobility Backend as a Service
+ Monitoring as a Service
+ Network Access Control as a Service
+ Network as a Service
+ Operations as a Service
+ Optimization as a Service
+ Payment as a Service
+ Quality as a Service
+ Query as a Service
+ Recovery as a Service
+ Remote Backup as a Service
+ Risk Assessment as a Service
+ Robot as a Service
+ Security as a service
+ Service Desk as a Service
+ Solutions as a Service
+ Storage as a Service
+ Telepresence as a Service
+ Test environment as a Service
+ Testing as a Service
+ Transport as a Service
+ Unified Communications as a Service
+ User Interface as a Service
+ Video Conferencing as a Service
+ Video Surveillance as a Service
+ Voice as a Service
+ Website as a Service

+ **Mélytanulás**
+ **Kvantumszámítástechnika**

3. ábra: Szolgáltatások a felhőben
Forrás: Koczka Ferenc, okosóra előadása az OTP Bank Nyrt-ben

A felhő alapú technológiát a rossz célokra, például a kiberbűnözők is igénybe tudják venni szakmai tudás nélkül is, erre jó példák az alábbiak:

- PhaaS Phishing as a service.
  - PhpaaS Phishing protection as a service.
- VaaS virus as a service.
  - VPaaS virus protection as a service.
- MaaS malware as a service.
  - MPaaS malware protection as a service.
- SaaS spam as a service.
  - SFaaS spam filter as a service.

– Any hacking as a service.

A FELHŐSZOLGÁLTATÁSOK IGÉNYBEVÉTELÉNEK SZEMPONTJAI

A felhőmegoldások igénybe vételekor számos esetben tapasztalható, hogy előre nem kerülnek részletes elemzésre a saját tulajdonú és üzemeltetési esetekhez képest a műszaki, a jogi, és az információbiztonsági szempontok, valamint nem készül kockázatelemzés sem. A felhőbe költözéssel kapcsolatban a döntést minden szervezetnek a saját működési folyamatait, valamint az azokra hatással lévő kockázatokat a kapcsolatos gazdasági hatásokkal együtt elemezve szükséges meghozni. A következőkben pár olyan szempontot ismertetünk, amelyet kiemelten fontosnak tartunk ehhez.

Késleltetések figyelembe vétele

Egy informatikai rendszer tervezésekor a felhasználó általi érzékeléstől, például a képernyőtől, az adatig oda és vissza szükséges az adatáramlásokat tervezni. Ezek alapján lehet meghatározni azon időértékeket, amelyek elérésekor egy folyamatot, műveletet meg kell szakítani[8]. Egy felhő komponenst nem tartalmazó esetben a modellben lévő minden szakaszra az elemi késleltetés (latency) jól számolható, a hálózatokok, szerverek, adattárolókon, felhasználói eszközökön stb. a műveleti idő. Ammenyiben egy felhasználó nem ugyanazon a helyi hálózaton van, mint a szerver, akkor az adatátvitelt biztosító távközlési szolgáltató (a továbbiakban: TELKO) által vállalt maximális mértéket szükséges figyelembe venni. Egy felhős szolgálatatás esetében sokszor Magyarország határain túl vannak a szerverek és számos IT ökoszisztéma elem. A TELKO-k az adatátvitel műszaki paramétereire az országhatáron belül vállalnak maximális késleltetési értéket, a nemzetközi szakaszokra nem. Amennyiben olyan folyamatokat működtet egy szervezet, amelyeken a késleltetés kritikus, például az azonnali fizetési rendszer, akkor az adatátviteli késleltetések bizonytalansága miatt célszérű lehet egy, a késleltetésre is garanciákat tartalmazó nemzetközi közvetlen adatkapcsolatot kiépíteni a felhőszolgáltatóhoz.

Skálázódás

A felhőben üzemeltett informatikai megoldásoknak egyik előnye, hogy az automatikus skálázódással mindig annyi erőforrás áll rendelkezésre, amennyi az adott pillanatban szükséges. Az alapműködés túl minden folyamat azonnal megkapja az igényelt erőforrását. Egy ilyen folyamat lehet rosszindulatú is, például egy vírus helyreállíthatatlan töröl, vagy írja felül az adatainkat. Emiatt egy kibertámadási folyamat is sokkal gyorsabban futhat le egy felhős megoldáson, ezzel jelentősen csökkentve az érzékelésre, reagálásra rendelkezésre álló időt. Célszerű definiálni a szervezet által validáltan indított folyamatokat és mindenképp szükséges a „végtelen” helyett maximált erőforrás igénybe vételére szerződni. Egy felhőszolgáltató a szerződésében vállalhatja korlátok nélküli erőforrások biztosítását, de valóságban számára is

[8] Time-out

korlátos erőforrás áll rendelkezésre. Azokban az esetekben, amikor a kapacitását meghaladó igény érkezik, akkor a nem valós idejű szolgáltatásaiból servereket vonhat el. Emiatt azokban pillanatnyi vagy tartósabb szolgáltatás kiesés tapasztalható. A jelenség folyamatos és mérhető. Ennek hatására alakultak ki szolgálatásokat mérő publikus megoldások, amelyek közül a legismertebb a https://downdetector.com/. A kibertér ma már elfogadottan hadműveleti tér a földön, vízen, levegőn, világűrön túl. A kiberműveletekhez szükséges erőforrások is biztosíthatók a felhőszolgálatók által mind a támadók, mind a védekezők számára. Tegyük fel a kérdést, hogy amennyiben egy kiberműveleti feladathoz és a szervezetünktől érkezik egyszerre többlet erőforrás igény egy nemzetközi felhőszolgáltatóhoz, akkor milyen döntés születik az erőforrások allokációjára? Egy kormány, egy haderő, vagy egy igénybe vevő szervezet kapja meg a rendelkezésre álló szabad erőforrást? Egy ilyen döntésben mekkora súlya lehet egy ügyfélnek, egy nemzetnek? A kérdésekre a válaszokat jelenleg kutatjuk még, de az eddig tapasztaltak alapján lehetőség szerint a hibrid felhő szolgálatói megoldás javasolt. Ebben az esetben az erőforrások egy része az igénybevevőnél van saját tulajdonban, azaz azok semmilyen esetben sem vonható el a működése fenttartásából. Ebben az esetben is a felhő technológia összes előnye megmarad.

Adatok rendelkezésre állása

A munkaszervezetek napi működése ma már elképzelhetetlen adatok nélkül. Amennyiben egy felhőszolgálatás és/vagy a kapcsolatos távközlési szolgáltató nem érhető el, akkor is birtokunkban kell legyen a szervezet egyik legnagyobb értéke az adatvagyon. Az MNB ajánlás 48. e) pontjában szerepel, hogy a mentett állományoknak a felhőszolgálatótól független is szükséges meglenniük kockázatarányosan[9]. A rendelkezésre álló adatokkal a működés fenntartását előre modellezni szükséges. Abból, hogy hogy pár LTO-14[10] szalagon fizikailag rendelkezésre áll az adatvagyon még nem következik, hogy a szervezet működéshez rendelkezésre állnak az adatok. Az üzletmenet-folytonossági (BCP) tervek készítése során szükséges olyan szcenárió kidolgozása is, amelyben a rendelkezésre álló adatokból kell az elvárt időn belül egy új helyen a szervezet működéséhez szükséges informatikai szolgálatásokat helyreállítani. Erre megoldás lehet egy másik felhőszolgálató igénybe vétele is. A modellezés során nem csak egy szolgálatás kiesésre célszerű a forgatókönyveket előre elkészíteni, hanem arra az esetre is, amikor a szervezet az adott felhőszolgálatás igénybe vételét valamilyen okból meg kívánja szüntetni. Ezen forgatókönyveket a szerződések megkötése előtt szükséges elkészíteni, annak érdekében, hogy az ehhez szükséges műszaki, gazdasági, jogi feltételeket a szerződés eleve tartalmazza.

[9] A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről

[10] Linear Tape-Open mágneses szalag 576 Terrabyte alap, kompresszió előtt 1,44 Petabyte kapacitással

Bizalmi elemek

Minden esetben fontos szempont az adatok bizalmasságának kialakítása, amelyhez minden adatot titkosítottan célszerű kezelni, és titkosított adatkapcsolatokon áramoltani. Az ehhez szükséges bizalmi elemek (kulcsok, titkosítási eszközök és szoftverek, eljárások) is az igénybe vevő által kezelten működhet, mert ebben az esetben alakítható ki teljes körűen a bizalmasság a felhőszolgáltatóval szemben is.

A szolgáltató ellenőrzése

A felhőszolgáltatók szolgáltatási csomagjaiban általában elérhetőek a szolgáltatás minőségét, az információbiztonságot ellenőrző alkalmazások is. Amennyiben kizárólag ezeket használjuk, akkor ezen komponensek üzemét lehetőség szerint saját üzemeltetésben lássuk el, mert ezzel csökkenteni lehet a kiszolgáltatottságot a szolgáltató felé. A működéssel, biztonsággal kapcsolatos összes adatot a szolgáltatótól független helyen is célszerű tárolni, és ezen a helyen saját eszközökkel feldolgozni.

Audit

Számos szervezet olyan tevékenységet végez, amely hatósági engedély köteles, a hatóság részéről folyamatosan felügyelt, az informatikai rendszerek folyamatos audit alatt állnak. Egy felhőszolgálatás használatakor ezeket is figyelembe kell venni. Ehhez a javasolt módszer az, hogy a szerződéskötés előtt meg kell győződni a kapcsolatos jogszabályokban, felügyeleti szerv előírásaiban, az audit módszertanokban előírt kontrollokról, például a 41/2015. (VII. 15.) BM rendeletben[11] szereplőkről. Ehhez el lehet fogadni a felhőszolgáltató által független harmadik féltől készített audit jelentéseket, azokat megfeleltetve kontroll szinten. A szolgatatóknál végzett auditok részletes dokumentációit tapasztatunk szerint nem publikálják, de megfelelő titoktartási megállapodás alapján megismerhetők.

Jogi szempontok

A felhőszolgáltatások igénybe vételének alapvető jogi akadálya nincs. Az Európai Unióban (EU) az adatkezelésre vonatkozó szabályok szerint az EU-n kívüli adattovábbításnak plusz garanciális feltételi vannak. A nagyobb felhő szolgáltatók emiatt is rendelkeznek EU-n belüli adatközpontokkal így nem valósul meg az EU-n kívüli adattovábbítás. A felhőben kezelt adatok esetében a kezelés tényét javasoljuk rögzíteni az adatvagyon leltárba is. Ekkor az adatok jellege miatti további előírások azonosíthatók. Amennyiben egy adat személyes adat akkor a felhőszolgáltatóval adatfeldolgozási megállapodást is létre kell hozni. Amennyiben egy adat pénzügyi ágazatban szabályozott adat például bank, biztosítási titokkörben van, akkor az ezek kezelésével kapcsolatos szerződési garanciákat biztosítani kell. Az adatok tartalma, jellege által

[11] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

vezérelt jogi szempontokra nagyon sok példát lehetne még írni. A jogi szempontokat már korai szakaszban tervezni kell. Amikor az érintett adatkörök összeállnak, akkor célszerűnek tartom az igénybe vevő szervezet jogi, adatvédelmi szakemberei által egy elemzésben összefoglalni a jogi szempontokat, amelyeket pont úgy kell figyelembe venni, mint a műszaki, biztonsági, gazdasági szempontokat. A létfontosságú rendszerelemet működtető szervezetek esetében az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény geolokációs előírása szerint az EU-ban lehet minden informatikai rendszer. A nemzeti adatvagyont kezelő szervezetek esetében hazánkban lehet.

A 2022-ben indult Orosz-Ukrán háború hívta fel a figyelmet arra, hogy gazdasági szankció része lehet olyan intézkedés is, amikor sok tízmillió magánszemély, több tízezer vállalkozás számára válnak elérhetetlenné a működésükhöz szükséges alapvetően szükséges felhő szolgáltatások még akkor is, ha a megkötött szerződés minden pontját betartották, a díjakat időben fizették és semmilyen okot nem adtak arra, hogy a szolgáltató egyoldalúan azonnali hatállyal felmondja a megállapodást. Ezt az esetet is figyelembe véve, amikor csak lehetséges hibrid szolgálatatásra javasolt a kötelmijogi megállapodást kialakítani a szolgáltatóval.

ÖSSZEFOGLALÁS

A felhőszolgáltatások igénybe vétele ma már gyakori minden magánszemély számára, aki mobileszközt használ. A szervezetek, közigazgatási szervek esetében a használat középtávon nem lesz elkerülhető. Amennyiben a használat előtt a jogi, műszaki, információbiztonsági, üzletmenet-folytonossági, tulajdonosi, kivonási, szempontokat elemezve választjuk ki a szolgáltatót, a működés alatt folyamatosan vizsgáljuk, akkor kockázatok jelentős mértékben csökkenthetők, de teljesen nem szüntethetők meg, ugyanúgy ahogyan a saját üzemeltetésben lévő rendszerek esetében sem.

FELHASZNÁLT FORRÁSOK

[1] *Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről, 2022. december 14.*

[2] *Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, 2022. december 14.*

[3] *Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete a pénzügyi ágazat digitális működési rezilienciájáról, 2022. december 14.*

[4] Peter Mall és Tim Grance, „U.S. Department of Commerce, National Institute of Standards and Technology," September 2011. https://csrc.nist.gov/publications/detail/sp/800-145/final, Letöltve: 2023. május 10.

[5] *A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről https://www.mnb.hu/letoltes/4-2019-felho.pdf*

[6] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

[7] *Special Publication 800-145, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf*

[8] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény

Military and Intelligence CyberSecurity Research Paper 2023/1.

Szerző(k) / Author(s):
Oláh István – Magyar Sándor

Kézirat lezárásának ideje / Manuscript closing time:
2023.08.15.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD
Dr. Magyar Sánor PhD

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Dr. Magyar Sándor PhD

Elérhetőségek /Contacts:
https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/researchpaper

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:
2786-3778

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.