HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 1. szám 101–120.
DOI: 10.32567/hm.2024.1.6

Hunorfi Péter,[1] Paráda István,[2] Farkas Tibor[3]

Kiberbiztonsági kihívások a légi közlekedésben – Kronológiai folyamat a Boeing elleni kibertámadások tükrében

Cybersecurity Issues in Aviation – Timeline of Cyber Crimes against Boeing

Absztrakt

Jelen cikkben a szerzők bemutatják a légi közlekedés egyik információs alrendszerét, informatikai megoldását, valamint annak potenciális kibertéri veszélyeit és kockázatait. Ehhez a szerzők egy elemző-értékelő módszerrel meghatározzák a légi közlekedés bizonyos informatikai elemeit, elsősorban a kommunikációs, adatkapcsolati és fedélzeti repülési rendszereket, például az úgynevezett electronic flight bag-eket (EFB), amelyek kiberincidensek következtében kiemelt jelentőségűek. Ezt követően a szerzők ismertetik a Boeing vállalatnál a közelmúltban bekövetkezett kibertámadásokat, illetve azok kronológiai sorrendjét, majd mindezeket összegezve logikai következtetéseket vonnak le azok hatásairól, illetve a támadás elleni fellépések újabb formájáról.

Kulcsszavak: légi közlekedés, EFB, NOTAMS, Boeing, kibervédelem, ransomware

[1] Doktori hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: hunorfi.peter@phd.uni-obuda.hu
[2] CIS Operations Officer, NATO Support and Procurement Agency, e-mail: paradaistvan@gmail.com
[3] Egyetemi docens, Óbudai Egyetem, e-mail: farkas.tibor@bgk.uni-obuda.hu

Abstract

In this article, the authors present an information subsystem of air transport, its IT solution, as well as its potential cyber threats and risks. To this end, the authors determine certain IT components of air transport with particular regard to communication, data link, and onboard flight systems, such as the so-called electronic flight bags (EFB), which have special significance due to cyber incidents. Following this, the authors describe the cyber attacks that occurred recently at Boeing, including their chronological order, and then, by summarising all these, they inductively draw logical conclusions about their impacts, as well as about new forms of response against the attacks.

Keywords: aviation, EFB, NOTAMS, Boeing, Cyber Defense, Ransomware

Bevezetés

Napjainkban a legtöbb kereskedelmi repülőgép innovatív technológiákat, rendszereket és példátlan infrastruktúrát használ a kibertechnológiákat is magában foglaló repüléselektronikai alkalmazásokhoz. A repülőgépek utasai ma már komplex informatikai rendszereket vesznek igénybe jegyvásárláskor, a repüléshez történő bejelentkezéskor, a repülőtéri biztonsági ellenőrzésen való áthaladáskor, valamint a nyílt, publikus internethez wifi és a beépített fedélzeti szórakoztató rendszerhez való csatlakozáskor. A kapcsolódó kibertechnológiák és a kapcsolódási lehetőségek a repülést a kiberfenyegetések veszélyes világának teszik ki, amelyek komoly kihívást jelentenek egy esetleges támadás során, és amelyek megnehezítik a kockázatok megértését vagy meghatározását. Emellett az új szolgáltatások és rendszerek fejlesztésével folyamatosan nőnek a támadások felületei és lehetőségei.

A repülési ipar jelentős átalakuláson ment keresztül az információs technológiai (IT) megoldások integrálásával, különösen az EFB-rendszerek formájában. Ezek a megoldások forradalmasították a repülési műveleteket, digitális hozzáférést biztosítva a pilótáknak a kritikus információkhoz és erőforrásokhoz. A digitális rendszerekre való fokozott támaszkodás azonban olyan kiberbiztonsági kihívásokat is jelentett, amelyeket kezelni kell. Ez a cikk a légi közlekedésben alkalmazott EFB-megoldásokhoz kapcsolódó kiberbiztonsági kihívásokat tárja fel, különösen a Boeing vállalatot ért kibertámadások szemszögéből. A repülőterek és a légi járművek elleni kibertámadások lehetősége valódi veszélyeket rejt magában, úgymint a földi és légi infrastruktúrák folyamatos és zökkenőmentes működtetésének akadályozása; az üzembiztonság sérülése; az adatok illetéktelen kezekbe kerülése vagy az informatikai és kommunikációs rendszerek összeomlása. A lehetséges kockázatok, az üzembiztonságra gyakorolt hatás és a szükséges mérséklő intézkedések vizsgálatával jobban megérthetjük a kiberbiztonság jelentőségét a légi közlekedés keretében.

A cikk legfontosabb kutatási kérdése, hogy a légi közlekedésben az Electronic Flight Bag (EFB) rendszerek és a kapcsolódó informatikai infrastruktúra kiberbiztonsági sebezhetőségeinek és fenyegetéseinek azonosítása, elemzése és kezelése milyen kihívásokat tartogat. A probléma magában foglalja a kiberfenyegetések változó

természetének megértését, a légi közlekedési ágazatra jellemző különleges biztonsági kockázatokat és a hatékony védelmi stratégiák kidolgozását a légi közlekedési ágazat egyedi igényeinek megfelelően. A Boeing vállalatnál bekövetkezett kibertámadások példáját felhasználva a kutatás célja az, hogy átfogó képet adjon az EFB-rendszerek potenciális kiberbiztonsági sebezhetőségeiről, azok lehetséges következményeiről a légi közlekedési műveletekre, valamint a megelőzés és a reagálás hatékony módszereiről.

A kutatás során alapvetően két hipotézis fogalmazható meg.

- (HT 1.) Az EFB-rendszerek integrációjának és a növekvő digitalizációnak köszönhetően a légi közlekedési ágazat egyre nagyobb kockázatnak van kitéve a kiberfenyegetésekkel szemben, ami jelentősen befolyásolhatja a repülésbiztonságot és az üzemeltetést. Ezen kiberfenyegetések kezelése érdekében a fejlett kiberbiztonsági protokollok és a személyzet folyamatos oktatása kulcsfontosságú lehet az EFB-rendszerek és a kapcsolódó informatikai infrastruktúra védelmében.
- (HT 2.) A Boeing vállalatot ért kibertámadások elemzése rávilágíthat arra, hogy a légitársaságok és a repülési szolgáltatások számára szükséges az EFB-rendszerek és a kapcsolódó informatikai infrastruktúra kiberbiztonsági kockázatainak proaktív kezelése, beleértve a rendszeres sebezhetőségi felülvizsgálatokat és a kiberbiztonsági incidensre való reagálási tervek kidolgozását. Az ilyen intézkedések jelentős mértékben csökkenthetik a kibertámadásokból eredő károkat, és biztosíthatják a légi közlekedés folyamatos és biztonságos működését.

A kutatás során alkalmazott módszertanként elsődlegesen a nemzetközi és a kevésbé jellemző hazai releváns szakirodalmak és információt biztosító oldalak feldolgozásával az EFB-rendszerek használatát, valamint működésének jellegét határozzuk meg. Ezt követően bemutatjuk a közelmúltban történt releváns kiberincidenseket kronológiai sorrendben, majd ajánlásokat teszünk a kockázatok lehetséges csökkentésére.

Informatikai és műveleti rendszerek a civil légi közlekedésben

Mára a kiberműveletek és a kibertámadások átszövik az élet minden területét. Nem képez kivételt ez alól a repülés, a légiirányítás, a repülőterek elleni támadások, illetve az ezen támadások elleni védelem sem.[4] A repülés teljes folyamata során alkalmazott rendszereket, szolgáltatásokat számos szempont szerint lehet csoportosítani:

- repülőgépek, repüléshez kapcsolódó eszközök, rendszerek (repülőgépek és elektronikai rendszerei, radarok, radarrendszerek, világítórendszerek stb.) tervezése, gyártása, üzemeltetése;
- repülőtéri utaskezelés (induló- és átszállójegy, valamint poggyász kezelése, beszállókártya és más forgalmi vonatkozások: repülőgép súly- és egyensúlyszámítása, rakodástervezés, konténeres rendezés, utashely foglalása, tarifálás, jegykiállítás);

[4] Szabó–Tóth 2013: 89–113.

- légiáru *(cargo)* helyfoglalása, tarifálás, okmányolás, raktári funkciók, járat-előkészítés, különleges árukategóriák, valamint a cargo kapcsolatrendszere a nemzetközi ügynökségi disztribúcióval, vámmal, repülőtéri funkciókkal stb.;
- légitársasági és repülőtéri automatizálás (nemzetközi poggyászkeresés és adminisztráció, utast és poggyászt összekötő és biztonsági megfeleltető megoldások, fizikai poggyászosztályozás és -irányítás, járatinformációs rendszerek);
- légitársasági operatív üzemirányítás: útvonal- és hálózattervezés, menetrend- és géprotáció-tervezés, menetrendszerkesztés és napi operatív menetrendi funkciók, repülőgépek műszaki karbantartásának tervezése és termelésirányítási rendszerek, hajózószemélyzet-tervezés és -vezénylés, navigációs rendszerek (útvonal- és üzemanyag-tervezés, repülési feltételek vizsgálata, például meteorológia), digitális föld-levegő kapcsolat.[5]

Ahogyan az az osztályozásból kikövetkeztethető, minden rendszerben megtalálható az informatika, az üzemeltetés nélkülözhetetlen alkotórésze az információs rendszer, amelynek számos eleme befolyásolható lehet, akár egy részegység működésének átprogramozásával, akár egy teljes rendszerbe történő behatolással, a rendszer irányításának átvételével. Fontos, hogy egy ilyen rendszer, a társaság vagy a szervezet méretétől függően, akár az egész világra is kiterjedhet. Mindenképpen mérlegelni kell azt is, hogy a fenti rendszerek különböző, más szervezetek által üzemeltetett elemekkel, hálózatokkal vannak kapcsolatban. Az ezekben lévő informatikai hiányosságok, illetve az ezek ellen indított támadások hatása befolyásolja a kapcsolódó egyéb rendszereket, szolgáltatásokat, ezáltal a repülést is.[6]

EFB

A pilótáknak rengeteg dokumentumot és információt kell ismerniük a repülés tartalmától függően. Ezen dokumentumok egy részének a repülés során fizikailag is elérhetőnek kell lennie. Ezek a fizikailag kötelező dokumentumok főként a repülőgép üzemeltetési kézikönyveit és a vészhelyzeti ellenőrző listákat, a teljesítményre és a súlyegyensúlyra vonatkozó irányelveket tartalmazzák. Ezenkívül vannak repülési dokumentumok is, amelyek a repülni kívánt útvonaltól és a leszálló gépeket fogadó repülőterektől függően változnak. Ezek a repülési dokumentumok tartalmazzák a légitársaság térképeit, a le- és felszállási területek süllyedési tervét, valamint a tartalék és vészleszállási területek süllyedési terveit is. Mindez rengeteg mappát eredményez, amelyeket a pilótáknak magukkal kell vinniük és használniuk.

A tablettechnológiák fejlesztése és a polgári légi közlekedési hatóságok általi használat eredményeként a repülési műveletekhez elérhetővé váltak az úgynevezett electronic flight bag-ek (EFB), amit magyar nyelvre leginkább „elektronikus repülőtáskának" lehetne fordítani. A légi úti térképeket és a leszállópályákat nyomtatott papírként előállító cégek most a „papírmentes pilótafülke" koncepcióra váltanak

[5] Gonda 2005: 14–15.
[6] Horváth 2020.

az általuk tervezett szoftverrel. Ahogy már fentebb szó volt róla, hagyományosan a pilóták papíron kapták meg a szükséges információkat. Manapság ezek az információk digitális formában vannak jelen. Az ilyen digitális adatok eléréséhez megkezdték a repülőgéprendszerekbe beágyazott vagy hordozható táblagépek alkalmazását. Az EFB név a pilóták által hordozott hagyományos repülőtáskákból ered, amelyek rengeteg papíralapú repülési ellenőrző listát tartalmaztak, repülési és időjárási térképeket, kézikönyvek köteteit.[7] A navigációs térképek, kézikönyvek és tanácsok létfontosságú források a repülési műveletekhez, főként a repülés kritikus szakaszaiban.[8] Ezeknek a dokumentumoknak a repülés közben gyorsan hozzáférhetőnek kell lenniük, mégpedig a repülésbiztonság veszélyeztetése nélkül. Az érintőképernyős eszközök megjelenése együttműködésre motiválta a repülőgépgyártókat és a repüléskezelő szoftverekre szakosodott szoftverfejlesztőket, mint például a Jeppesen, a ForeFlight és a Garmin cégeket. Együtt megoldásokat dolgoztak ki a papíralapú űrlapok elektronikus másolatokra való áttelepítésére.[9] A szoftverfejlesztők migrálták a repülőgép-dokumentumok papíralapú változatait, és integrálták a repülőgépteljesítmény-alkalmazásokat egy elektronikus platformba, amely táblagépeken lett elérhető.[10]

1. ábra: Boeing Jeppesen ForeFlight Mobile EFB mobil applikáció
Forrás: https://d32dgjuo8qzfhk.cloudfront.net/assets/foreflight_mobile_hero_www.png

7 Ateş 2017.
8 Babb 2017a.
9 Ohme 2014.
10 Babb 2017b.

Ezeknek a rendszereknek köszönhetően jelentősen csökkent a pilóták és a hajózószemélyzet fizikai terhelése. Az elektronikus repülőtáskák költséghatékonyak és felhasználóbarátak. Az új fejlesztéseknek és szabályoknak megfelelően felhasznált dokumentumok folyamatosan frissülnek. A pilótáknak a repülés megkezdése előtt meg kell győződniük arról, hogy az általuk használt dokumentumok minden módosítása frissült. Az összes dokumentum gyors elérése külön kihívást jelent.[11]

Az EFB közvetítő szerepet tölt be a pilóta és a légi közlekedésben részt vevő civil és katonai szervezetek, illetve társaságok között azáltal, hogy átláthatóvá teszi a légi járművek működési nyilvántartásait. Lehetőséget biztosít a pilótafeladat-folyamatok vagy validálások digitalizálására, valamint megakadályozhatja a dokumentumok elvesztését is. Továbbá a Global Position Systems (GPS) beépítésével az EFB-be a pilóták megtekinthetik a mozgó repülőtéri térképeket, ami csökkentheti a pilóták munkaterhét.[12]

Összességében az EFB a hagyományos papíralapú repülési anyagok digitális megfelelője. Hatékony hozzáférést biztosít az információk széles köréhez, ezáltal javítja a repülés előtti tervezést és a repülés közbeni műveleteket. Az EFB-k döntő szerepet játszanak a légi közlekedés modernizálásában, javítva a hatékonyságot, a biztonságot és a kényelmet a pilóták és a légitársaságok számára egyaránt. A komplex, hatékony előnyök mellett számos kockázatot is rejt a rendszer. Mint minden technikai eszköz, az EFB esetében is számolni kell hardver- és szoftverhibával. A műszaki jellegű hibák mellett a szabályozási kérdések és a technológiai függőség is jelentős lehet. A téma szempontjából a tárolt információk biztonságának szerepe kulcsfontosságú, ennek információ- és kiberbiztonsági megközelítése elengedhetetlen.

NOTAM

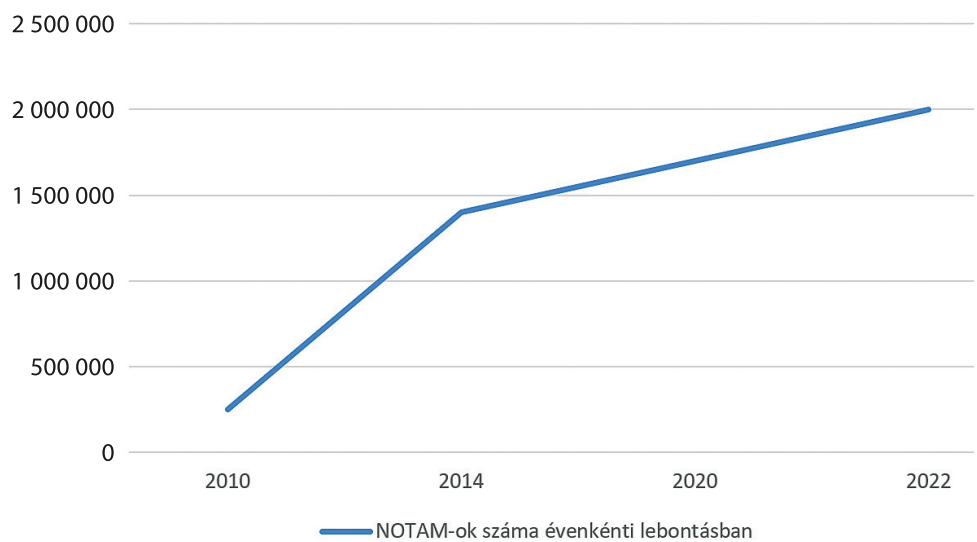
A NOTAM *(Notice to Airmen)* egy iparági kifejezés a légi közlekedési hatóságok által kiadott értesítésekre, amelyek célja a pilóták figyelmeztetése a repülési útvonalon felmerülő lehetséges veszélyekre. A légügyi hatóságok által kiadott közlemény rendeltetése a pilóták és más repülőszemélyzet tájékoztatása a légtér, a repülőterek vagy a navigációs eszközök, berendezések működésével kapcsolatos fontos információkról. A NOTAM-ok olyan lényeges információkat tartalmaznak, amelyek befolyásolhatják a repülés biztonságát, például a kifutópályák elérhetőségének változásáról, ideiglenes repülési korlátozásokról, navigációs segédeszközök kieséséről vagy a repülési útvonalon lévő veszélyekről. A veszélyekről szóló értesítések közzétételének elmulasztása kockázatot jelenthet a repülőgépekre és a repülésbiztonságra.[13] A Szövetségi Légi Közlekedési Hivatal (Federal Aviation Administration, FAA) szerint, amely az USA közlekedési minisztériumán belül működő ügynökség, a NOTAM olyan információkat tartalmaz, amelyek alapvető fontosságúak a repülést üzemeltető személyzet számára, és amelyek nem voltak ismertek eléggé előre ahhoz, hogy más módon terjeszthessék.

[11] Özkan–Aksoy–Şensoy 2021.
[12] Suppiah et al. 2020.
[13] Boeing Subsidiary Jeppesen Suffers Cyberattack 2023.

Értesíti a pilótákat különösen a Nemzeti Légtérrendszer (National Airspace System, NAS)[14] valamely összetevőjének rendellenes állapotáról. A NOTAM-okat az FAA számos különböző okból bocsátja ki, de elsősorban azért, hogy tájékoztassák a pilótákat a repülőtereket, a légi utakat és a helyi eljárásokat érintő változásokról, amelyek hatással lehetnek a személyzet vagy a földön tartózkodók biztonságára. Sokféle NOTAM létezik, beleértve a nemzetközi, a hazai, a katonai és a polgári NOTAM-okat. Lehetnek tanácsadó jellegűek vagy kötelező utasítások.[15]

Mindezek alapján látható, hogy a NOTAM-ok létfontosságúak a repüléstervezés és a biztonságos repülés lebonyolítása szempontjából, mivel valós idejű tájékoztatást nyújtanak a repülési műveleteket befolyásoló körülményekről. A pilótáknak minden repülés előtt át kell nézniük a NOTAM-okat, hogy tisztában legyenek a légtérben bekövetkező változásokkal vagy veszélyekkel. Ennek megfelelően az információk biztonsága kiemelt fontosságú, az esetleges incidensek beláthatatlan következményekkel járhatnak.

A NOTAM-ok száma évről évre folyamatosan növekszik. Míg 2010-ben 250 ezer NOTAM-ról beszélhettünk, ez a szám 2022-re meghaladta a kétmilliót.



2. ábra: A nemzetközi NOTAM-ok számának alakulása 2010–2022 között
Forrás: a szerzők szerkesztése PUFAHL *2022 alapján*[16]

[14] A NAS alatt az Egyesült Államok légterét, navigációs létesítményeit és repülőtereit, a hozzájuk kapcsolódó szolgáltatásokat és valamennyi szabályt, előírást, eljárást értjük, az ide tartozó személyzettel és felszerelésekkel együtt.
[15] *A repülésben használt NOTAM-ok különböző típusai* [é. n.].
[16] Global NOTAM Campaing 2022.

Az EFB-k kiberbiztonsági tényezői

Az EFB-megoldások számos előnnyel járnak, ugyanakkor érzékenyek a kiberbiztonsági sebezhetőségekkel és fenyegetésekkel szemben. E kihívások megértése alapvető fontosságú a légi közlekedési műveletek védelme szempontjából. Az EFB-rendszerekben lévő sebezhetőségek és veszélyek három fontosabb terület köré sorakoztathatók fel.

Az első a *külső kibertámadások.* Az EFB-rendszerek potenciális célpontjai a sebezhetőségeket kihasználni, jogosulatlan hozzáférést szerezni, adatokat manipulálni vagy a műveleteket megzavarni kívánó rosszindulatú szereplőknek.

A második terület a *belső fenyegetések és emberi tényezők.* A humán tényező olyan kockázatokat hordoz magában, mint például a nem szándékos hibák, hanyagság vagy szándékos, rosszindulatú tevékenységek, visszaélések az EFB-rendszerekhez magas hozzáféréssel rendelkező „bennfentesektől".

A harmadik terület az *adatszivárgás és jogosulatlan hozzáférés*. Az EFB-k érzékeny információkat tárolnak, beleértve az előzőekben már említett repülési terveket, az utasok jegyzékeit és a repülőgép teljesítményadatait, amelyek miatt vonzó célpontok a kiberbűnözők számára.

Az üzembiztonságra gyakorolt lehetséges hatásait szintén három alapvető területre lehet bontani: Az egyik a *repülési adatok és navigációs rendszerek manipulálása.* Az EFB-ket célzó kibertámadások manipulálhatják a repülési adatokat, a navigációs térképeket, vagy akár megváltoztathatják a kritikus repülési paramétereket, ami helytelen repülési pályákhoz, a helyzetfelismerés megsértéséhez és potenciális repülésbiztonsági veszélyekhez vezethet.

A második a *kommunikációs rendszerek kompromittálása*. Az EFB-k kommunikációs csatornákra támaszkodnak valós idejű időjárás-frissítések, légi forgalmi irányítási kommunikáció és egyéb kritikus információk érdekében. Az ilyen rendszerek megsértése megzavarhatja a kommunikációt és veszélyeztetheti az üzembiztonságot.

A harmadik pedig az *EFB működésének megzavarása*. A kiberbiztonsági incidensek, mint például a rosszindulatú programok fertőzései vagy a szolgáltatásmegtagadási támadások, megzavarhatják az EFB-rendszerek működését, akadályozva a repülési műveleteket, és befolyásolhatják a járatok, repülések általános biztonságát és hatékonyságát.

A kiberbiztonsági és információbiztonsági kockázatok mérséklése érdekében a légitársaságoknak és a légi közlekedési hatóságoknak szilárd biztonsági intézkedéseket kell bevezetniük, beleértve a titkosítást, a hitelesítést, a hozzáférés ellenőrzését, a behatolásjelző rendszereket és a rendszeres biztonsági ellenőrzéseket. Emellett a pilóták és a személyzet számára szervezett folyamatos kiberbiztonsági tudatossági képzés elengedhetetlen a biztonsági tudatosság előmozdításához a légi közlekedési ágazatban. A légi forgalmi társaságok ellen irányuló kibertámadások jelentős kockázatot jelentenek a repülésbiztonságra, az üzemeltetés integritására és az utasok bizalmára nézve. Az ágazatban az alábbi alapvető kockázatok, támadási formák okoznak, okozhatnak problémát.

Alapvető veszélyt jelentenek az *adatvédelmi incidensek.* Az EFB-k az előzőekben meghatározott, repüléssel kapcsolatos érzékeny információkat tárolnak, beleértve a navigációs térképeket, repülési terveket és üzemeltetési adatokat. Ha ezek az eszközök

nincsenek megfelelően biztosítva, akkor sérülhetnek az adatok, ami a bizalmas információkhoz való jogosulatlan hozzáférést vagy azok ellopását eredményezheti.

Az egyéb, általános célú információs rendszerekhez hasonlóan a *rosszindulatú programok és vírusok* hasonló veszélyt jelentenek. Az EFB-k, mint minden elektronikus eszköz, fogékonyak a rosszindulatú szoftverekre és vírusokra. Ha egy EFB megfertőződik, az veszélyeztetheti a repülési adatok integritását, megzavarhatja a működést, vagy lehetővé teheti a támadók számára, hogy jogosulatlanul hozzáférjenek a kritikus rendszerekhez.

Ehhez kapcsolódik a *jogosulatlan hozzáférés*. A gyenge hozzáférés-ellenőrzés vagy a nem megfelelő hitelesítési mechanizmusok lehetővé tehetik, hogy illetéktelen személyek hozzáférjenek az EFB-khez vagy a rajtuk tárolt érzékeny információkhoz. Ez a repülési tervek, navigációs adatok vagy más kritikus rendszerek jogosulatlan módosításához vezethet.

A *szolgáltatásmegtagadás-alapú támadások (DoS)* alapvetően korlátozhatják az információkhoz való hozzáférést. Az EFB-k a valós idejű adatokhoz, időjárás-frissítésekhez és egyéb szolgáltatásokhoz való hozzáféréshez hálózati kapcsolatra támaszkodnak. A szolgáltatásmegtagadásos támadás megszakíthatja a kapcsolatot, megakadályozva a pilótákat abban, hogy repülés közben hozzáférjenek az alapvető információkhoz, ezzel befolyásolva a helyzetfelismerést és a döntéshozatalt. A kibertérből érkező fenyegetések mellett fontos figyelembe venni a *fizikai biztonsági kockázatokat*. Az EFB-k olyan hordozható eszközök, amelyeket a pilóták a repülőgép fedélzetén hordoznak. Tehát ha egy EFB elveszik, ellopják vagy manipulálják, az potenciálisan veszélyeztetheti az érzékeny információkat, vagy biztonsági réseket hozhat létre a légi közlekedés ökoszisztémájában. Az utolsó kiemelt terület az *ellátási lánc kockázatai*. Az EFB-k különböző gyártóktól származó hardverkomponensekből és szoftveralkalmazásokból állnak. Az ellátási lánc kockázatai, például a hamisított alkatrészek, a rosszindulatú firmware vagy a nem biztonságos szoftverek olyan sebezhetőségeket hozhatnak létre az EFB-kben, amelyeket a támadók kihasználhatnak.

Az előzőekben leírtak jól alátámasztják, hogy a komplex védelmi tevékenységek elengedhetetlenek a fent említett, kiemelt támadások ellen. Az információbiztonság minden részterületére kiemelt hangsúlyt kell fektetni, amelyek mára már nemcsak a repülőgépekre mint eszközökre vonatkoznak, hanem a teljes kapcsolódó infrastruktúrára, rendszerekre és személyi állományra is.

A Boeing multinacionális vállalatot ért kibertámadások

Az előzőekben felsorolt veszélyforrások, támadási módszerek egyéb repülési rendszereket vagy a légi közlekedéshez köthető alrendszereket is fenyegetnek. Amennyiben a támadók hozzáférést szereznek a kritikus repülési rendszerekhez, manipulálhatják a navigációs vezérlőket, megváltoztathatják a repülési útvonalakat, megzavarhatják a fedélzeti rendszereket. Az ilyen támadások a repülőgép feletti irányítás elvesztését, a levegőben történő baleseteket vagy engedély nélküli leszállást eredményezhetnek.

A repülési társaságok hatalmas mennyiségű érzékeny információt tárolnak, beleértve az utasok adatait, a repülési menetrendeket és az üzemeltetési részleteket.

Az adatszivárgás személyes információk, pénzügyi adatok vagy védett üzleti adatok nyilvánosságra kerüléséhez vezethet, ami károsíthatja a vállalat hírnevét, és pénzügyi veszteségeket okozhat.

A légitársaságok foglalási rendszereit, járattervezési szoftvereit vagy kommunikációs hálózatait célzó kibertámadások megzavarhatják a járatok működését, ami járatkésésekhez, járattörlésekhez vagy logisztikai kihívásokhoz vezethet. Ezek a zavarok a teljes légi közlekedési ökoszisztémára hatással lehetnek, több érdekelt felet érintve és jelentős gazdasági hatást okozva. A 3. ábra a légi közlekedési iparhoz köthető, 2022-ben történt kibertámadásokat mutatja be.

3. ábra: Légiiparhoz köthető kiberincidensek 2022-ben
Forrás: a szerzők saját szerkesztése, online: https://konbriefing.com/en-files/cyber-attacks/2022-ind-aviation-tl-en.png [17]

A KonBriefing Research 2022-re vonatkozóan összesen 114 sikeres kibertámadást azonosított az alábbi iparágak vállalatai és szervezetei ellen: repülés (38); közlekedés (32);

[17] KonBriefing 2022.

repülőterek (21); légitársaságok (10); repülés és védelem (4); közszféra (2); katonaság (2); egyetemek (1); technológia (1); szolgáltatók (1); mentés (1); egészségügy (1).[18]

A leggyakoribb általános támadási formák a légi közlekedéshez kapcsolódóan is megjelennek. A zsarolóprogram-támadások kritikus rendszereket vagy adatokat titkosíthatnak, és a visszafejtésért a támadók pénzt követelnek. Ha a repülőcégek rendszereit zsarolóvírusos támadás éri, az működési leálláshoz, pénzügyi veszteségekhez és hírnévkárosodáshoz vezethet. Emellett fennáll a veszélye annak, hogy a váltságdíj kifizetése esetén is érzékeny információk kerülnek nyilvánosságra. Social engineering technikákat vagy adathalász e-maileket szintén használhatnak a támadók, hogy a repülőtársaságok alkalmazottait, pilótáit vagy az érzékeny rendszerekhez hozzáféréssel rendelkező személyzetet célba vegyék. Ha ezek a támadások sikeresek, akkor az rendszerekhez való jogosulatlan hozzáférést, adatlopást vagy rosszindulatú szoftverek telepítését eredményezheti.

Az elmúlt néhány évben a nemzetközi repülőterek földi és légi infrastruktúrájának működtetése egyre bonyolultabb technológiákat, automatizált rendszereket követelt, ami megnövelte a repülőterek és a légi közlekedési ágazat sérülékenységét a számítógépes bűnözőkkel és a terroristákkal, valamint azon bennfentes alkalmazottakkal szemben, akik az adatok ellopásával, a kritikus infrastruktúrák működési biztonságának akadályozásával zavart, bizonytalanságot, fennakadásokat kívánnak kelteni. Ezeket az állapotokat a járvány okozta helyzet még tovább súlyosbította. A légi közlekedési ágazat informatikai beruházásainak szintje 2014–2019 között 21,4 milliárd dollárról 35,2 milliárd dollárra növekedett. A teljes IKT- (információs és kommunikációs technológia) beruházásokon belül a kiberbiztonság növelését célzó fejlesztések aránya 2016-ban 4,6%; 2017-ben 7%; 2018-ban 9% és 2019-ben 14% volt.[19] A repülőterek kiberfenyegetettségekkel szembeni ellenállásának javítása azonban nem kizárólag a pénzügyi forrásokon múlik, ehhez az egyes repülőterek kiberbiztonsági érettségi szintjét is növelni szükséges. Ezen szemléletváltáshoz a járvány utóhatásai valószínűleg hozzá fognak járulni. Szükségeltetik egy tudatos kiberbiztonsági politika megfogalmazása a kockázatok rendszeres feltérképezésével és beazonosításával; információk, kiberbiztonsági incidensek, tapasztalatok, tanulságok, legjobb gyakorlatok kölcsönös megosztásával; valamint a hálózatos együttműködés kiépítése és megfelelő szabályozási környezet kialakítása a munkavállalók érzékenyítésével és a kiberbiztonsági tudatossági szint képzésekkel, tréningekkel történő emelésével.

Boeing-kiberincidens, 2018

A Boeing vállalatot 2018 márciusában érte WannaCry vírusos informatikai támadás. A Microsoft Windows XP szoftverének gyengeségeit kihasználva az úgynevezett WannaCry kibertámadás világszerte széles körű zavarokat okozott. Több százezer számítógépet fertőzött meg. Célja, hogy megakadályozza a felhasználók adatokhoz való hozzáférését, amíg váltságdíjat nem fizetnek, gyakran kriptovalutában.

[18] Cyber Attacks on the Aviation Industry in 2022. Statistics: Ransomware, Data Breaches, DDoS Attacks 2023.
[19] Florent 2020.

A vírus elsőként 2017. május 12-én jelent meg, és képes volt gyorsan terjedni a Windows operációs rendszereket futtató számítógépek között. A zsarolóvírus-támadás az évtized egyik legpusztítóbbja volt, több mint 150 országban érintett magánszemélyeket és szervezeteket. Megbénította az Egyesült Királyság kórházait, leállította a gyártósorokat, és felborította az emberek életét. A spanyol Telefónica távközlési vállalat az elsők között számolt be a támadásról, majd gyorsan terjedt Európa számos országában.

A Microsoft javításokat bocsátott ki a sebezhetőség orvoslására, habár egyes vállalatok, mint például Corey Nachreiner, a WatchGuard Technologies technológiai igazgatója szerint, óvakodnak a gyakori frissítésektől, attól tartva, hogy ez veszélyeztetheti egyedi rendszereiket. A Microsoft nem kívánta kommentálni a Boeing elleni kibertámadást.[20]

A támadás kezdetben aggodalmat keltett a Boeing vállalaton belül, különösen azért, mert attól féltek, hogy a vírus kárt tehet a kulcsfontosságú repülőgépgyártási eszközökben. Ennek ellenére a vállalat vezetése hamarosan közölte, hogy sikerült minimalizálniuk a támadás okozta károkat.

A helyzet napközben jelentős aggodalmat váltott ki mind a Boeing munkatársai, mind a légitársaságok között, de estére a vállalat megnyugtatást adott. Linda Mills, a Boeing Commercial Airplanes kommunikációs igazgatója kijelentette: „Elvégeztük a végső értékelést" – utalva arra, hogy a probléma csupán néhány gépet érintett, és hogy szoftverfrissítésekkel sikerült orvosolniuk a helyzetet. „Nem érintette a 777-es jet programját vagy bármely más programunkat." Mike VanderWel, a vállalat gyártásmérnöki részlegének vezetője az események kezdetén figyelmeztető üzenetet küldött, amely komoly aggodalmakat vetett fel, de ezek a félelmek alaptalannak bizonyultak.

A délutáni órákban a Boeing hivatalos közleményt adott ki, amelyben Mills elmagyarázta a helyzet kezeléséhez szükséges lépéseket, beleértve az IT-csapat teljes körű bevonását és a tények pontos azonosítását. Ebben a közleményben arra is rámutatott, hogy a kiberbiztonsági műveleti központ csak korlátozott számú rosszindulatú program behatolását észlelte, amit sikeresen kezeltek anélkül, hogy ez bármilyen termelési vagy szállítási problémát okozott volna.

Boeing-kiberincidens, 2022

A Jeppesen, amely vállalat a Boeing teljes tulajdonában áll, élen jár a légi navigációs szolgáltatások terén. Navigációs adatbázisokat, repüléstervezési alkalmazásokat kínál EFB-khez, valamint portfóliójába tartozik a NOTAM-kezelés is.

2022. november 2-án több Jeppesen-szolgáltatás is leállásra kényszerült, ami a következő figyelmeztetés megjelenését eredményezte a vállalat weboldalán (4. ábra):

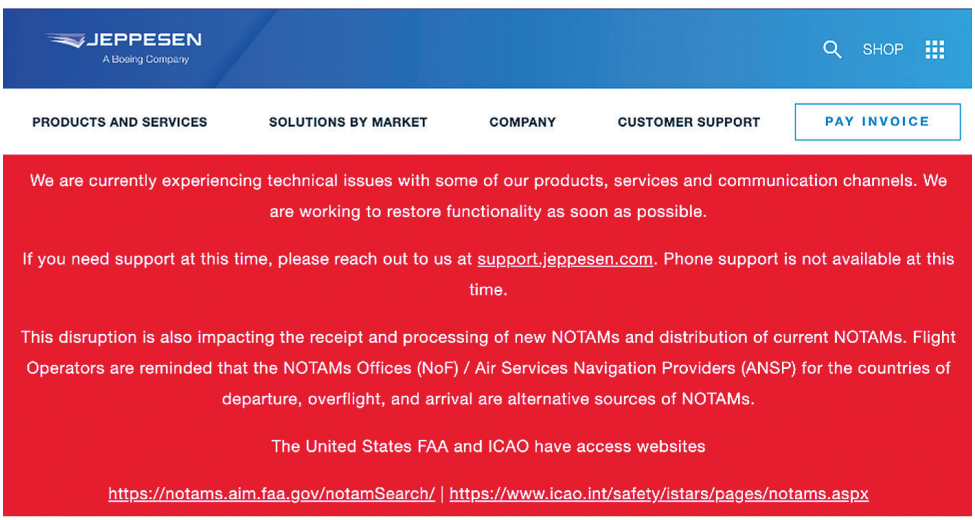
„Jelenleg technikai problémákat tapasztalunk egyes termékeinkkel, szolgáltatásainkkal és kommunikációs csatornáinkkal kapcsolatban. Dolgozunk a működőképesség mielőbbi

[20] Gates 2018.

helyreállításán. Ha jelenleg segítségre van szüksége, forduljon hozzánk a support.jeppesen.com címen. Telefonos támogatás jelenleg nem érhető el."[21]

A Boeing hivatalos közleményében a következőképpen nyilatkozott:

„Leányvállalatunk, a Jeppesen, kiberincidenst tapasztalt, amely bizonyos repüléstervezési termékeket és szolgáltatásokat érintett. A repüléstervezésben némi fennakadás történt, de jelenleg nincs okunk azt hinni, hogy ez az incidens veszélyt jelentene a repülőgépekre. Folyamatosan kommunikálunk az ügyfelekkel és a szabályozó hatóságokkal, és azon dolgozunk, hogy a lehető leghamarabb helyreállítsuk a teljes körű szolgáltatást."[22]



4. ábra: Jeppesen-közlemény a kibertámadás miatt nem működő elemekre, mint például a NOTAM
Forrás: Zee 2022

A támadás természetét, a károk kiterjedését, egyéb részleteket, valamint a helyreállítás várható időpontját a Boeing akkor nem kívánta ismertetni, és később sem mutattak be részletesebb információkat az ügyről.

A kibertámadás a légi közlekedés tekintetében jelentős kockázatokkal járhat, amelyekre fel kell készíteni és megfelelően támogatni a repülőgép-személyzetet és a légi közlekedéshez köthető valamennyi résztvevőt. Az FAA által kiadott, úgynevezett FAA Advisory Circular 90-100A az üzemeltetéshez kapcsolódó, útvonalakra, eljárásokra és egyéb üzemeltetéshez köthető szabványokra, szabályokra vonatkozó „tanácsadó körlevél", kiadvány. Ezek tájékoztató jellegűek, nem kötelező érvényű ajánlások. Az AC 90-100A szerint a fedélzeti navigációs adatoknak naprakésznek és a tervezett műveleti régióval összhangban kell lenniük, beleértve a navigációs segédeszközöket,

[21] Klint 2022.
[22] Thurber 2022.

útpontokat és a terminálra vonatkozó eljárásokat.[23] Mindehhez kapcsolódik Rich Pickett pilótának, a Personal Wings Inc. munkatársának a kiberincidenshez fűzött megjegyzése is:

„Ha a pilóta VFR[24]-es, noha előfordulhat biztonsági probléma a lejárt GPS-adatbázissal való repülés során, attól még VFR esetében ez nem előírás. Az IFR[25] esetében előírás. Az adatbázisnak aktuálisnak kell lennie, vagy más forrásból, például az FAA-grafikonokból leellenőrzöttnek kell lennie. Az IFR-terminálejárások esetében az FAA-diagramokkal való keresztellenőrzéssel ellenőrizniük kell, hogy az eljárások nem változtak-e az előző ciklushoz képest. Ha az útpont adatai megváltoztak, a pilóta nem használhatja az RNAV[26] megközelítést. A keresztezési magasságok és minimumok változásai azonban jelentős biztonsági problémákat okozhatnak, különösen a robotpilótával összekapcsolt megközelítéseknél. Más szavakkal: növeli a pilóták munkáját, és hatással van a biztonságra."[27]

A kiberbiztonság továbbra is jelentős aggodalom forrása a légi közlekedésben. A szolgáltatásmegtagadási támadásoktól – amelyek több repülőtéri weboldalt is érintettek – egészen a légitársaságokat célzó zsarolóvírus-támadásokig. Az Európai Légiközlekedés-biztonsági Szervezet 2021-es jelentése szerint a kibertámadások száma minden fenyegetési kategóriában nőtt, ami éves szinten 530%-os emelkedést jelent.[28]

Boeing-kiberincidens, 2023

2023. október 27-én a Boeing neve megjelent a LockBit weboldalán, ahol november 2-ig adtak időt a vállalatnak a kapcsolatfelvételre és a tárgyalások megkezdésére annak érdekében, hogy ne kerüljenek nyilvánosságra adatok komoly károkat okozva. A csoportnak nagy mennyiségű érzékenynek minősített adatot sikerült megszereznie.

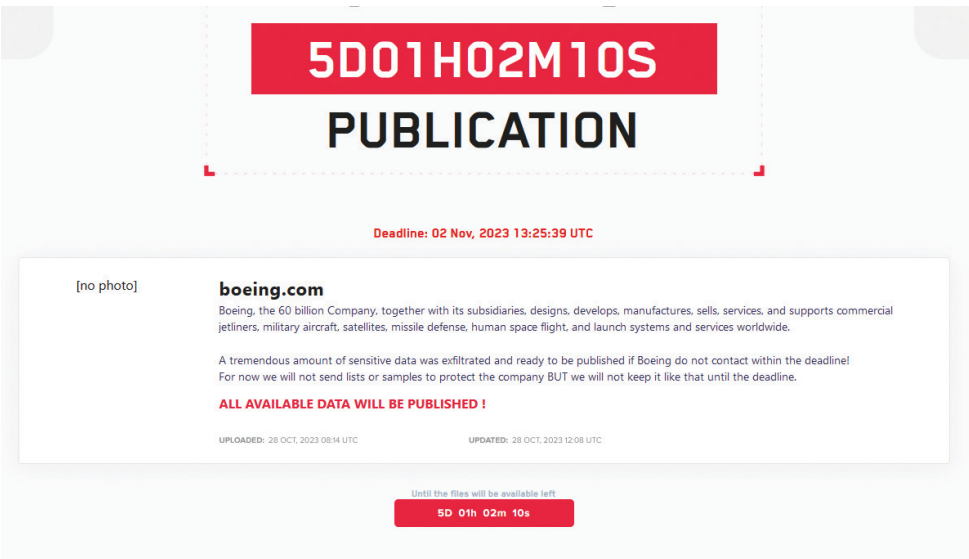
Egy rövid időre a Boeing eltűnt a LockBit áldozatainak listájáról, de november 7-én ismét felkerült, amikor a csoport kijelentette, hogy figyelmeztetéseiket figyelmen kívül hagyta a cég. November 10-én a LockBit közzétette a weboldalán a Boeingtől származó összes adatot, amelyek között IT-menedzsment-szoftverek biztonsági mentései, monitoring- és auditeszközök naplói találhatók. A hackercsoport közel 50 GB adatot szivárogtatott ki a Boeingtől, miután az nem volt hajlandó fizetni. A kiszivárogtatott információk nagy része biztonsági mentés volt, ezek között szerepeltek 2023. október 22-én készültek is.

A szivárgásban szereplő Citrix eszközök biztonsági mentései arra utalnak, hogy a LockBit kihasználhatta a Citrix Bleed sebezhetőségét (CVE-2023-4966), ennek igazolására október 24-én jelentek meg bizonyítékok.

[23] U.S. Department of Transportation 2015.
[24] VFR: Visual Flight Rules – „látvarepülési" szabályok, vizuális repülési szabályok.
[25] IFR: Instrument Flight Rules (műszeres repülési szabályok).
[26] RNAV: Area Navigation (területi navigáció).
[27] Personal Wings 2022.
[28] Britton 2022.

A Boeing megerősítette, hogy kibertámadás érte őket, de ebben az esetben sem árult el részleteket arról, hogyan történt a „betörés". A vállalat kiemelte, hogy a kiberbiztonsági incidens most sem veszélyezteti a repülésbiztonságot, és aktívan együttműködnek a bűnüldöző és szabályozó hatóságokkal az eset kivizsgálásában. A Boeing biztosította ügyfeleit, hogy a támadás nem érintette repülőgépeik működését, viszont továbbra is kérdéses maradt, hogy a hackerek pontosan mennyi adatot szereztek meg.[29]

A LockBit csoport ransomware-as-a-service (RaaS) szolgáltatást nyújt, több mint négy éve aktívan okoz károkat különböző szektorokban, az autóipartól kezdve a postai szolgáltatásokig. Az Egyesült Államok kormánya szerint a csoport 2020 és 2023 között több mint 1700 támadással közel 91 millió dollárt zsarolt ki, de tevékenységük globális szinten is jelentős. Például 2023 augusztusában a spanyol rendőrség figyelmeztetett egy LockBit által végrehajtott adathalászati kampányra, amely spanyol építőipari vállalatokat vett célba.[30]



5. ábra: Boeing-zsarolás a LockBit adatszivárgási oldalon
Forrás: Gatlan 2023

Kutatási eredmények

A Boeinget ért kiberbiztonsági incidensek rávilágítanak a nagyvállalatok előtt álló jelentős kihívásokra és kockázatokra, amelyekkel kényes információik és kritikus rendszereik kiberfenyegetésekkel szembeni védelme során szembesülnek. A kibertámadások kockázatának mérséklése érdekében a repülési vállalatoknak prioritásként

[29] Raj 2023.
[30] Ilascu 2023.

kell kezelniük a kiberbiztonsági intézkedéseket, például a robusztus hálózati biztonsági protokollok bevezetését, a szoftverek és rendszerek rendszeres frissítését, a munkavállalók kiberbiztonsági képzését, valamint az iparági partnerekkel való együttműködést a fenyegetésekkel kapcsolatos információk és a legjobb gyakorlatok megosztása érdekében. Emellett a szabályozó hatóságok döntő szerepet játszanak a kiberbiztonsági előírások betartatásában és a kiberbiztonsági kultúra előmozdításában a légi közlekedési ágazaton belül. Összességében tehát a kibertámadásokból levont következtetések kiemelik, hogy fontos a kibervédelem, a felkészültség minden részterületének folyamatos javítása a mai digitális környezetben működő szervezetek számára.

Lényeges továbbá kiemelni, hogy a Boeing az olyan vállalatok egyike, amelyek a polgári életben alkalmazott légi járművek gyártása mellett a védelmi iparban is jelentős szerepet játszanak repülőgépek, helikopterek, rakéták, műholdak és egyéb védelmi rendszerek tervezésével és gyártásával. Ezt figyelembe véve a kibertámadások elleni küzdelem hangsúlyosabbá válása vitathatatlan.

A Boeing által elszenvedett kibertámadások élesen emlékeztetnek arra, hogy a kritikus légi közlekedési infrastruktúra védelme, valamint a légi közlekedés biztonságának és védelmének biztosítása érdekében az egyre inkább digitalizálódó világban sürgősen átfogó kiberbiztonsági stratégiákra van szükség.

Az előzek alapján mit tehetünk, amikor egy partnercég kibertámadás áldozatává válik, és ez potenciálisan érinti a saját szervezet biztonságát vagy működését? Több kiberbiztonsági ellenlépést is meg kell fontolni annak érdekében, hogy minimalizáljuk a károkat, és megőrizzük a saját rendszereink integritását. Az alábbi néhány lépést érdemes végrehajtani, amelyek általános érvényűek szakterülettől függetlenül:

1. Azonnali értesítés és kommunikáció
   - Értesítse a saját kiberbiztonsági csapatát vagy szolgáltatóját a partnercég kibertámadásáról.
   - Létesítsen kommunikációs csatornát a partnercég és a saját szervezete között a támadással kapcsolatos információk és frissítések megosztására.
2. Hálózati elszigetelés
   - Izolálja azokat a hálózati szegmenseket, rendszereket vagy alkalmazásokat, amelyek közvetlenül kapcsolatban állnak a támadás által érintett partnerrel, hogy megakadályozza a potenciális kártékony tevékenységek terjedését.
3. Hozzáférés ellenőrzése és ideiglenes korlátozások
   - Ideiglenesen korlátozza vagy szüntesse meg a partnercég hozzáférését a saját hálózatához és rendszereihez, amíg a biztonsági kockázatokat fel nem mérjük és kezeljük.
   - Ellenőrizze és szigorítsa a hozzáférés-vezérlési szabályokat, beleértve a tűzfalakat, a VPN-eket és más határvédelmi eszközöket.
4. Biztonsági felülvizsgálat és sebezhetőségi ellenőrzés
   - Végezzen átfogó biztonsági felülvizsgálatot és sebezhetőségi szkennelést a saját rendszereken, hogy azonosítsa és orvosolja az esetleges gyengeségeket.
   - Győződjön meg arról, hogy a rendszerek naprakészek, és hogy az összes releváns biztonsági javítást alkalmazták.
5. Incidensreagálási terv aktiválása

- Aktiválja a saját incidensreagálási tervét, amely magában foglalja a lépéseket a potenciális fertőzések azonosítására, izolálására és megszüntetésére.
- Készítsen részletes naplózást és dokumentációt az eseményekről és a hozott intézkedésekről a későbbi vizsgálat és felülvizsgálat érdekében.

6. Biztonsági oktatás és tudatosság
- Informálja a dolgozókat a partnercég kibertámadásáról és annak potenciális hatásairól a saját szervezetre.
- Hangsúlyozza a biztonsági legjobb gyakorlatokat és az óvatosságot, különösen a gyanús e-mailekkel és kommunikációkkal kapcsolatban.

7. Jogi és szabályozási követelmények
- Konzultáljon jogi és szabályozási szakértőkkel a támadás jelentésével és a szükséges intézkedésekkel kapcsolatban.
- Ellenőrizze, hogy vannak-e kötelezettségek az adatvédelmi törvények és szabályozások alapján.

Összegzés, következtetések

A légi forgalmi infrastruktúrát célzó kibertámadások, köztük az olyan incidensek, mint a Boeing Jeppesen leányvállalata elleni támadás, aláhúzzák a légi közlekedési rendszerek kritikus sebezhetőségét a rosszindulatú szereplőkkel szemben. Az ilyen támadások jelentős kockázatot jelentenek a repülésbiztonságra, az üzemeltetés integritására és az utasok bizalmára. A Jeppesenhez hasonló, a légi navigációs szolgáltatásokat érintő támadások aggályokat vetnek fel a repüléstervezés, a navigációs térképek és a kritikus üzemeltetési adatok biztonságával kapcsolatban. Továbbá a repülési társaságokat célzó támadások megzavarhatják a működést, járatkésésekhez vagy járattörlésekhez vezethetnek, és gazdasági hatást gyakorolhatnak az egész légi közlekedési ökoszisztémára.

Mivel a légi közlekedési ágazat egyre inkább az EFB-megoldásokra támaszkodik, a kiberbiztonság fontosságát nem lehet túlbecsülni ezen a területen. A légi közlekedés és a Boeing mint ilyen tevékenységű vállalat sajátos kiberbiztonsági kihívásokkal néz szembe, amelyeket hatékonyan kell kezelni a repülések sikere, a műveleti biztonság és az érzékeny információk védelme érdekében. Hatékony biztonsági intézkedések bevezetésével, az együttműködés elősegítésével és a feltörekvő technológiák által nyújtott lehetőségek kihasználásával a légi közlekedési ipar hatékonyan mérsékelheti a kiberbiztonsági fenyegetéseket, és erősítheti az IT-s EFB-megoldások rugalmasságát.

A ransomware támadások hatásának minimalizálása érdekében a szervezeteknek javasolt rendszeresen biztonsági másolatot készíteni adataikról, és a biztonságos másolatokat offline állapotban tartani. Továbbá rendkívül fontos a rendszerek frissítésekkel és vírusirtó szoftverekkel való ellátása, azok frissítése. Ezeket a frissítéseket javasolt a szervezeten belül egy erre dedikált folyamatba ágyazni, vagy magát a folyamatot létrehozni és rendszeresen ellenőrizni azok végrehajtását, kontroll alatt tartását.[31]

[31] Tóth 2022: 192.

Ahogy a kiberfenyegetések folyamatosan fejlődnek,[32] az EFB kiberbiztonságának folyamatos fejlesztésére és javítására van szükség. A jövőbeni fejlesztések egyik területe a mesterséges intelligencia és a gépi tanulási algoritmusok integrációja a kiberfenyegetések észlelésének és a reagálásnak a javítása érdekében. Mindkettő segíthet javítani a légi közlekedési szervezetek azon képességét, hogy valós időben észleljék a kiberfenyegetéseket, és gyorsan reagáljanak rájuk. Például a hálózati forgalmi adatok elemzésével ezek az algoritmusok szokatlan tevékenységi mintákat észlelhetnek, amelyek egy folyamatban lévő kibertámadásra utalhatnak.

Ezenkívül a biztonságos kommunikációs protokollok és a fejlett hitelesítési mechanizmusok fejlesztése az EFB-k biztonságát is növelheti. Ezek a mechanizmusok segíthetnek megakadályozni az EFB-khez való jogosulatlan hozzáférést, és biztosítják, hogy csak az arra feljogosított személyzet férhessen hozzá az érzékeny adatokhoz.

Ahogy a légi közlekedési ipar folyamatosan fejlődik és felkarolja a digitális technológiát, az EFB kiberbiztonsági jelentősége csak nőni fog. A kiberbiztonságba való befektetéssel és a felmerülő fenyegetésekkel való szembenézéssel a légi közlekedési ágazat továbbra is biztonságos repülést biztosíthat az utasok számára szerte a világon.

Felhasznált irodalom

A repülésben használt NOTAM-ok különböző típusai [é. n.]. Online: https://hu.motonoticias.com/different-types-notams-used-aviation-82278

Ateş, Savaş Selahattin (2017): Electronic Flight Bag in the Operation of Airline Companies: Application in Turkey. *Computer Science and Information Technology,* 5(4), 128–134. Online: https://doi.org/10.13189/csit.2017.050402

Babb, Tyler A. (2017a): Professional Pilot Commercial Off-the-Shelf (COTS) EFB Usage, Policies and Reliability. *International Journal of Aviation, Aeronautics, and Aerospace,* 4(1), 1–29. Online: https://doi.org/10.15394/ijaaa.2017.1159

Babb, Tyler A. (2017b): Electronic Flight Bag Policies at Collegiate Aviation Programs. *International Journal of Aviation, Aeronautics, and Aerospace,* 4(4), 1–22. Online: https://doi.org/10.58940/2374-6793.1190

Boeing Subsidiary Jeppesen Suffers Cyberattack (2023). *Binary Defense,* 2023. április 18. Online: www.binarydefense.com/threat_watch/boeing-subsidiary-jeppesen-suffers-cyberattack/

Britton, Niki (2022): 'Cyber Incident' Affected Flight Planning. Boeing Subsidiary Jeppesen Apparently Targeted. *AOPA,* 2022. november 9. Online: www.aopa.org/news-and-media/all-news/2022/november/09/cyber-incident-affected-flight-planning

Cyber Attacks on the Aviation Industry in 2022. Statistics: Ransomware, Data Breaches, DDoS Attacks (2023). *KonBriefing,* 2023. február 28. Online: https://konbriefing.com/en-topics/cyber-attacks-2022-ind-aviation.html

Florent, R. (2020): Aerospace Cybersecurity: Building Resilience in the Hailstorm. *CyberInflight,* 2020. május 10. Online: www.cyberinflight.com/?p=1081

[32] Kovács 2023.

Gates, Dominic (2018): Boeing Hit by WannaCry Virus, But Says Sttack Caused Little Damage. *The Seattle Times,* 2018. március 28. Online: www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/

Gatlan, Sergiu (2023): Boeing Confirms Cyberattack Amid LockBit Ransomware Claims. *Bleeping Computer,* 2023. november 2. Online: www.bleepingcomputer.com/news/security/boeing-confirms-cyberattack-amid-lockbit-ransomware-claims/

Gonda Zsuzsanna (2005): *Repülési informatika.* Bicske: SZAK. Online: https://real.mtak.hu/170257/1/Gonda-Zsuzsanna-Repulesi-Informatika-konyv-SZAK-Kiado-2005-NJSZT-publikacio.pdf

Horváth József (2020): A repülés elleni kibertámadás. *Hadmérnök,* 15(3), 179–196. Online: https://doi.org/10.32567/hm.2020.3.10

Ilascu, Ionut (2023): LockBit Ransomware Leaks Gigabytes of Boeing Data. *Bleeping Computer,* 2023. november 12. Online: www.bleepingcomputer.com/news/security/lockbit-ransomware-leaks-gigabytes-of-boeing-data/

Klint, Matthew (2022): Breaking: Boeing's Jeppesen Subsidiary Hit with Potential Ransomware Attack. *Live and Let's Fly,* 2022. november 3. Online: https://live-andletsfly.com/boeing-jeppesen-ransomware-attack/

Kovács László (2023): *Hadviselés a 21. században: kiberműveletek.* Budapest: Ludovika.

Ohme, Marty (2014): Use of Tablet Computer as Electronic Flight Bags in General Aviation. *Aviation / Aeronautics / Aerospace International Research Conference,* 37. Online: https://commons.erau.edu/aircon/2014_Challenges_Facing_our_Industry/january-17-2014/37

Özkan, N. Fırat – Aksoy, Emre – Şensoy, Gökberk (2021): Evaluation of Jeppesen and Garmin Electronic Flight Bags (EFBs) Applications in Terms of Cognitive Workload and Availability. *International Journal of Multidisciplinary Studies and Innovative Technologies,* 5(1), 36–45. Online: https://dergipark.org.tr/en/download/article-file/1787377

Peredy Zoltán – Venczel Márk (2020): Nemzetközi repülőterek kiberbiztonsági kihívásai. *Repüléstudományi Közlemények,* 32(2), 165–180. Online: https://doi.org/10.32560/rk.2020.2.12

Personal Wings [@PersonalWings] (2022): Aviation Cyber Security and Recent Boeing Jeppesen Ransomware Hack. *YouTube,* 2022. november 6. Online: www.youtube.com/watch?v=RhLeTHTKxoU

Pufahl, Alexander (2022): *Global NOTAM Campaign.* Online: www.icao.int/NACC/Documents/Meetings/2022/AIMTF5/AIMTF5-P04.pdf

Raj, Aaron (2023): Boeing Hack: Should the Airline Manufacturer Negotiate with Cybercriminals? *Tech Wire Asia,* 2023. november 6. https://techwireasia.com/2023/11/boeing-hack-should-the-airline-manufacturer-negotiate-with-cybercriminals/

Suppiah, Saravanan et al. (2020): Impact of Electronic Flight Bag (EFB) on Single Pilot Performance and Workload. *International Journal of Aviation, Aeronautics, and Aerospace,* 7(4), 1–14. Online: https://doi.org/10.15394/ijaaa.2020.1531

Szabó Sándor – Tóth Rudolf (2013): Repülőterek kialakítása, létesítményeinek kritikus elemei, védelmük lehetséges műszaki megoldásai. *Repüléstudományi Közlemények,*

25(2), 89–113. Online: www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-07-Szabo_Sandor-Toth_Rudolf.pdf

THURBER, Matt (2022): Jeppesen Planning, Chart Products Suffer 'Technical Issues'. *AIN Online,* 2022. november 4. Online: www.ainonline.com/aviation-news/business-aviation/2022-11-04/jeppesen-planning-chart-products-suffer-technical-issues

TÓTH András (2022): *A digitális állam információbiztonsági kihívásai.* Budapest: Ludovika.

U.S. Department of Transportation (2015): *Federal Aviation Administration: Advisory Circular, 90-100A*. Online: www.faa.gov/documentLibrary/media/Advisory_Circular/AC_90-100A_CHG_2.pdf

ZEE, Mark (2022): Jetplanner, FD Pro, Charts – Down. *OPS Group,* 2022. november 3. Online: https://ops.group/blog/jetplanner-fd-pro-charts-down/