Ügyszám: NAIH-1245-29/2023
Előzmény: NAIH-8516/2022
Kapcs.: NAIH-8390/2022

Tárgy: döntés hivatalból induló adatvédelmi hatósági eljárásban

H A T Á R O Z A T

A **Nemzeti Adatvédelmi és Információszabadság Hatóság** (a továbbiakban: Hatóság) az **Educational Development Informatikai Zrt.** (2023. április 20. napját megelőzően: **eKRÉTA Informatikai Zrt.**) (székhely: 1111 Budapest, Budafoki út 59., cégjegyzékszám: 01-10-140310) (a továbbiakban: Ügyfél vagy Kötelezett) adatkezelésével kapcsolatban a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló (EU) 2016/679 rendelet (a továbbiakban: általános adatvédelmi rendelet) 32-34. cikkeinek feltételezhető megsértése miatt 2022. november 11. napján az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 60. § (1) bekezdése alapján hivatalból indított adatvédelmi hatósági eljárásban az Ügyféllel szemben az alábbi döntést hozza:

A Hatóság

megállapítja, hogy

1) a) a Kötelezett nem tett eleget az általános adatvédelmi rendelet 32. cikk (1) bekezdés b) pontjában, valamint a 32. cikk (2) bekezdésében foglalt kötelezettségének azzal, hogy az informatikai fejlesztői környezetének adatbiztonsági beállításai során nem vette kellőképpen figyelembe az adatkezelésből eredő olyan kockázatokat, amelyek a személyes adatok jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek, és emiatt a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét nem garantálta.

b) a Kötelezett nem tett eleget az általános adatvédelmi rendelet 33. cikk (2) bekezdésének azzal, hogy az adatvédelmi incidenst nem jelentette be indokolatlan késedelem nélkül az adatkezelőknek.

2) **utasítja a Kötelezettet**, hogy jelen határozat megállapításairól a határozat kézhezvételétől számított harminc napon belül tájékoztassa a köznevelési intézményeket (iskolákat), mint adatkezelőket.

3) az 1) pontban foglalt jogsértések miatt a Kötelezettet a jelen határozat véglegessé válásától számított 30 napon belül

110.000.000 Ft, azaz százötzmillió forint

adatvédelmi bírság megfizetésére kötelezi.

A bírságot a Hatóság központosított bevételek beszedési célelszámolási forintszámlája (10032000-01040425-00000000 Központosított beszedési számla IBAN: HU83 1003 2000 0104 0425 0000 0000) javára kell átutalással megfizetni. Az összeg átutalásakor a NAIH-1245/2023 BÍRS. számra kell hivatkozni.

Amennyiben a Kötelezett a bírságfizetési kötelezettségének határidőben nem tesz eleget, késedelmi pótlékot köteles fizetni. A késedelmi pótlék mértéke a törvényes kamat, amely a késedelemmel érintett naptári félév első napján érvényes jegybanki alapkamattal egyezik meg. A késedelmi pótlékot a Hatóság központosított bevételek beszedési célelszámolási forintszámlája (10032000-01040425-00000000 Központosított beszedési számla) javára kell megfizetni. A bírság és a késedelmi pótlék meg nem fizetése esetén a Hatóság elrendeli a bírság és a késedelmi pótlék végrehajtását.

Jelen határozattal szemben közigazgatási úton jogorvoslatnak nincs helye, de az a közléstől számított 30 napon belül a Fővárosi Törvényszékhez címzett keresetlevéllel közigazgatási perben megtámadható. A veszélyhelyzet a keresetindítási határidőt nem érinti. A keresetlevelet a Hatósághoz kell benyújtani, elektronikusan, amely azt az ügy irataival együtt továbbítja a bíróságnak. A tárgyalás tartása iránti kérelmet a keresetlevélben jelezni kell. A teljes személyes illetékmentességben nem részesülők számára a közigazgatási per illetéke 30 000 Ft, a per tárgyi illetékfeljegyzési jog alá esik. A Fővárosi Törvényszék előtti eljárásban a jogi képviselet kötelező.

INDOKOLÁS

I. Előzmények és a tényállás tisztázása

1. Jelen határozatban az Ügyfél vagy Kötelezett megjelölés alatt a 2023. április 20. napját megelőző tényállási elemekre vonatkozóan a Hatóság az eKRÉTA Informatikai Zrt.-t, azt követően az Educational Development Informatikai Zrt.-t érti. A névváltozástól eltekintve a Kötelezett egyéb adatai (székhely, cégjegyzékszám, adószám) a tárolt cégkivonat alapján változatlanok maradtak.

2. A Hatóság 2022. november 7. napján szerzett tudomást egy internetes hírportálon megjelent – a https://telex.hu/tech/2022/11/07/kreta-rendszer-e-naplo-kozoktatas-adathalasz-tamadas-adatszivargas-ekreta-informatikai-zrt webhelyen 2022. november 7. napján 10:30 perc óta elérhető – cikk alapján az eKRÉTA Informatikai Zrt.-t ért informatikai támadásról és adatvédelmi incidensről, majd ezt követően a hírekben foglaltak miatt, és mivel ezek megjelenését megelőzően nem kapott az Ügyféltől adatvédelmi incidensbejelentést, 2022. november 8. napján az általános adatvédelmi rendelet 32-34. cikkében foglalt kötelezettségek Ügyfél általi teljesítésének tárgyában hatósági ellenőrzést indított.

3. A linkelt cikkben többek között az alábbi állítások szerepelnek:

4. *„Néhány héttel ezelőtt adathalász támadás érte a Köznevelési Regisztrációs és Tanulmányi Alaprendszer, azaz a KRÉTA fejlesztőcégét, az eKRÉTA Informatikai Zrt.-t.*
A támadás sikeres volt, így a támadó illetéktelen hozzáférést szerezhetett a közoktatás minden intézményében kötelezően használt adminisztrációs rendszer adataihoz – értesült a Telex a cégtől független forrásból.
Úgy tudjuk, valamennyi diák összes, a KRÉTA-ban kezelt adata kiszivároghatott, de nemcsak ezekhez, hanem a cég más adatbázisaihoz és a forráskódokhoz, illetve a fejlesztők belső kommunikációjához is hozzáférhettek.
Információinkat névtelenül az eKRÉTA Zrt.-n belülről is megerősítették, a fejlesztésre rálátó forrásunk szerint valóban történt adathalász támadás: egy projektvezető kattintott egy fertőzött linkre egy átverős emailben, az ő adatait megszerezve férhettek hozzá belső adatbázisokhoz, és gyakorlatilag mindent elértek a cég rendszerein belül.

Úgy tudjuk, az eset még szeptemberben történt. Érdekesség, hogy a KRÉTA Tudásbázis nevű hivatalos információs oldalon a fejlesztőcéget ért adathalász támadással nagyjából egy időben, szeptember 20-i dátummal megjelent egy, cikkünk írásakor is az oldal tetején olvasható, „Fontos tájékoztatás!" című írás arról, hogy „az elmúlt időszakban újra megjelentek az adathalász alkalmazások (szoftverek), melyeket e-mailben és más csatornákon terjesztenek az adathalászok"."

5. *„A KRÉTA szélesebb körben elsősorban e-naplóként ismert, de mára egy komplett közoktatási informatikai rendszerré duzzadt. Ahogy a honlapján látható, összesen húszféle modul és különféle alkalmazások tartoznak hozzá, többek között olyan szolgáltatásokkal, mint az az e-napló, e-ellenőrző, intézményi adminisztrációs rendszer, digitális kollaborációs tér, e-ügyintézés, illetve egészségüggyel, étkeztetéssel, gazdálkodással, HR-ügyekkel kapcsolatos adminisztráció."*

6. A Hatóság a hatósági ellenőrzés megindítását követően megjelent további hírek – https://telex.hu/tech/2022/11/09/kreta-rendszer-ekreta-zrt-adathalasz-tamadas-adatszivargas-elhallgatas-naih-vizsgalat-eljaras és https://telex.hu/tech/2022/11/11/kreta-adatszivargas-forraskod-ekreta-zrt-fejlesztok-elvandorlas -, valamint az időközben a Hatóság felé az Ügyfél, illetve az egyes tankerületek által megküldött adatvédelmi incidensbejelentések ismeretében az általános adatvédelmi rendelet 32-34. cikkeinek feltételezhető megsértése miatt az Infotv. 60. § (1) bekezdése alapján 2022. november 11. napján hivatalból adatvédelmi hatósági eljárás indítása mellett döntött.

7. Idézetek a cikkekből, melyek linkjeit az előző bekezdés tartalmazza:

8. *„Helló, eKRÉTA! Sajnálatos módon a »profi« rendszereiteket sikeresen feltörtük, rengeteg adatot megszereztünk, köztük: forráskódok, adatbázisok, és még sorolhatnám! […] Mellesleg köszönjük a nagyon fontos, informatív Slack-beszélgetéseket, az újságíróknak biztos tetszeni fog, hogy a rendőröknek hamisítotok, stb" ez az üzenet a KRÉTA közoktatási adminisztrációs rendszert fejlesztő cég, az eKRÉTA Zrt. egy belső kommunikációs felületén köszöntötte a dolgozókat, miután a céget adathalász támadás érte: egy átverős emailben az egyik projektvezető rákattintott egy fertőzött linkre, és a támadók hozzáférést szereztek a rendszereikhez, többek között a KRÉTA által kezelt adatokhoz, illetve a fejlesztői adatbázisokhoz és kódokhoz is.*

9. *Ezt onnan tudjuk, hogy az adatszivárgást más forrásokra alapozva nyilvánosságra hozó cikkünk után felvette velünk a kapcsolatot a támadásban részt vevő egyik hekker, hogy további részleteket áruljon el."*

10. *„A belső kommunikációról hozzánk eljutott képek és szövegrészletek szerint az illetékesek sokat tanakodhattak arról, hogyan kezeljék a történteket. Egy projektvezetők közötti csetüzenetfolyam tanúsága szerint egyiküknek – a gyanús linkre kattintó, tehát a meghekkelt projektvezetőnek – feltűnt, hogy valaki olyan adminisztrátori hozzáféréssel végzett el egy változtatást, amelyhez vele együtt csak négyen ismerik a jelszót, és mivel négyük közül egyikük sem csinált ilyet, nem értették, mi történhetett."*

11. *„Még gázabb a dolog, mert a kérdéses üzenetek az után jöttek, hogy a Fori megváltoztatta a tanuló jelszavát" – írta később a projektvezető, amikor kezdett számukra kibontakozni, hogy nagyobb problémába futhattak bele. (A „Fori" az említett technikai adminisztrátori fiók, amelyhez a hekkerek hozzáfértek.) „Mi a fasz" – válaszolta erre a beszélgetés másik szereplője. „És az egésszel most mi a szart csinálunk? Balázs tudni sem akar róla – amit megértek…" – írta a projektvezető, feltehetően Szabó Balázsra, az eKRÉTA Zrt. vezérigazgatójára utalva, akit az előző cikkünk megjelenése előtt mi is többször kerestünk, de a cég központi elérhetőségeihez hasonlóan tőle sem érkezett emailben válasz, a telefont pedig nem vette fel."*

12. *„Egy másik üzenetben az adathalászat áldozatául esett projektvezető ezt írta valamivel később, szeptember végén:*
„A csütörtöki megbeszélésünk után maradt bennem rossz érzés, hogy megfelelően járunk-e el. Az egy fontos megállapítás volt részedről, hogy vagy végig igazat kell mondani, vagy végig tagadni, de menet közben nincs módosítási lehetőség. Azt szeretném, hogy tudd, hogy én tényleg nem tudok hazudni, de nem is szeretnék.”
Az adminisztrátori jogokkal bíró fiókról, amelynél felfedezték, hogy valaki hozzáférhetett, ezt írta: „[…] be lehet vállalni, hogy volt ilyen technikai felhasználónk, de az incidens után azonnal megszüntettük, ami teljesen igaz is. (Szeptember 18-án, vasárnap derült fény erre, azonnal jelszót változtattam, majd másnap töröltem az összes felhasználóbelépést – töröltre állítottam.) […] Ha ezt tagadnánk, neki meg lenne erre bizonyítéka (kép, videó, a tőlem letöltött belépési adatok, bármi), akkor kerülnénk abba a helyzetbe, amit mindenképpen el kellene kerülni.”
Ennek az utolsó levélnek a teljes szövegét, néhány képpel együtt, a hekkerek már közzétették hétfő este, azon a Telegram-csatornán, ahol a nekünk nyilatkozó társuk szerint további adatok publikálását tervezik.”

13. *„A hekkert arról is kérdeztük, hogyan sikerült bejutniuk az eKRÉTA rendszereibe. Állítása szerint egy általuk írt kártevő programot, egy úgynevezett RAT-ot (remote access trojan, azaz távoli hozzáférést lehetővé tevő trójai program) sikerült bejuttatniuk, méghozzá úgy, hogy az a cég minden vírusirtóján és védelmi szoftverén észrevétlenül átjutott. Ez a kártevőtípus épp arra jó, amire a neve utal: települ a megfertőzött rendszeren, és ezzel bejuttatja a támadókat is: távoli hozzáférést tesz lehetővé, ami jelentheti a rendszer távoli megfigyelését, de akár parancsok futtatását vagy adatok kinyerését is.*

14. *A trójait a KRÉTA üzenetküldő rendszerén keresztül terjesztették: kiválasztottak minden adminisztrátort, és egy megtévesztő adathalász (phishing) emailben, magukat másnak kiadva átküldték a kártevő letöltéséhez szükséges linket, olyasminek álcázva, ami felkeltheti a célba vett adminisztrátorok érdeklődését – mint azóta látjuk, egyikőjükét valóban fel is keltette. Az egyik projektvezető még azelőtt kattintott, hogy a cégen belül jelezték volna a dolgozóknak, hogy adathalász levelekről van szó, és ezzel sikerült megszerezniük a jelszavát, amellyel már mindenhez hozzá tudtak férni. „Nem volt kétlépcsős azonosítás, és egy rendszeren fut az egész, tehát ha van a owa.rufusz.hu-hoz hozzáférésed, akkor mindenhez is” – mondta a hekker. (A Rufusz Computer Informatika Zrt. annak a Fauszt Zoltánnak az egyik cége, akinek az érdekkörébe az eKRÉTA Zrt. is tartozik – erről előző cikkünk végén írtunk.)*

15. *Szeptember közepén még nem volt hozzáférésük a rendszerekhez, akkor még csak abba a már említett technikai adminisztrátori fiókba jutottak be, amely minden iskolában működött, de már ezzel is bármelyik tanulónak meg tudták nézni a lakcímét és más adatait. „Később jöttünk rá, hogy valójában van hozzáférésünk mindenhez: emailek, forráskódok stb.” A hekker állítása szerint végül tömörítve 238 GB adatot hoztak el a cégtől. A személyes adataikkal érintettek pontos számát nem tudják, de több tízezerről lehet szó.”*

16. *„Úgy tudjuk, hogy az eKRÉTA Zrt.-nél szeptemberben, miután tudomást szereztek magáról a hekkerek bejutásáról, még arra a megállapításra juthattak, hogy adatszivárgás nem történt (azt pedig pláne nem tudták, hogy a hekkerek még több mint egy hónappal később is a rendszereikben vannak). Az adatok kikerülésének nyomait csak az első cikkünk után találták meg, de ők úgy látták, hogy a támadók hozzáférése korlátozottabb volt.*
Azt hitték, csak ahhoz juthattak hozzá, ami az adathalász emaillel rászedett projektvezető gépén különféle okokból elérhető volt, a teljes rendszert nem – ami, ha bebizonyosodna, jó hír lenne, hiszen azt jelentené, hogy a gyakorlatban érintettek köre is jóval szűkebb lenne az elméletileg lehetségesnél. Mindezt hivatalos forrásból sajnos továbbra sem tudjuk megerősíteni, mert a cég

még egyetlen megkeresésünkre sem reagált semmilyen csatornán, amikor cikkeink megjelenése előtt a történtek tisztázására kértük."

17. 2022. november 10. napján tett adatvédelmi incidensbejelentésében az Ügyfél az alábbi információkat osztotta meg a Hatósággal.

18. Az Ügyfél 2022. november 7. napján, a támadónak az Ügyfél belső kommunikációra használt csatornáján közzétett bejegyzése által szerzett tudomást a támadásról, a támadó jelenlétéről. A közzétett bejegyzés alapján a támadó az Ügyfél belső fejlesztői környezeteihez, munkaszervezéshez és munkavégzéshez használt csatornáihoz hozzáfért, azokat megfigyelte.

19. A támadó több oktatási intézmény alkalmazottjainak kártékony kódot tartalmazó linkkel ellátott üzenetet küldött a KRÉTA rendszeren keresztül, és az ebben található linkre az Ügyfél egyik munkavállalója rákattintott. Ezzel a támadó bejutott és hosszabb ideig bent tartózkodott az érintett kolléga számítógépében, melyen keresztül hozzáférhetett az Ügyfélnél munkavégzéshez használt rendszerekhez, a számítógépen elmentve tárolt jelszavakhoz. Az incidens kb. 1.300.000 darab személyes adatot érinthetett, melyek kb. 100.000-150.000 fő felhasználóhoz (akik lehetnek felhasználói jogosultsággal rendelkező alkalmazottak, diákok, szülők) tartoznak.

20. Az érintettek tájékoztatásáról az Ügyfél a bejelentésben úgy nyilatkozott, hogy őket tájékoztatta / tájékoztatásukat tervezi, ahogyan a vizsgálatok függvényében ezt szükségesnek látják.

21. Az incidens észlelése után a felhasználó számítógépe újratelepítésre, az érintett felhasználói fiók pedig megszüntetésre került. A hálózaton belüli szolgáltatások biztonságának fokozása folyamatban volt (távoli elérés szigorítása, MFA, szükséges és elégséges jogosultságok felülvizsgálata, IT biztonsági érzékenyítés, képzés).

22. A hatósági eljárás során a Hatóság munkatársai *előzetes értesítés mellett* 2022. november 17. napján az Ügyféllel egyeztetett helyszínen, az Ügyfél központi ügyintézési helyén (1117 Budapest, Gábor Dénes utca 4.) helyszíni szemlét tartottak. A helyszín szemlét megelőzően az Ügyfél tájékoztatta a Hatóságot, hogy az éles KRÉTA rendszer tekintetében az IT infrastruktúra elemek a Klebelsberg Központ fenntartása alá tartozó köznevelési intézmények esetén a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-nél találhatók. Az Ügyfél belső fejlesztői környezeteire, munkaszervezésre és munkavégzésre használt belső csatornáira vonatkozóan a Rufusz Computer Informatika Informatikai Szolgáltató Zrt. (székhely: 1111 Budapest, Budafoki út 59., cégjegyzékszám: 01-10-140532) lát el adatfeldolgozói tevékenységet. A helyszíni szemle során a Hatóság által feltett kérdésekre az Ügyfél – többek között - az alábbi információkat szolgáltatta.

23. Az Ügyfél szoftverfejlesztéssel és szakértői tevékenység nyújtásával is foglalkozik. Ahogy érzékelték az incidenst [megj.: 2022 szeptember közepén], azonnal lecserélték az adathalász támadás áldozatául esett munkavállaló (a továbbiakban: érintett felhasználó) gépét, és inaktiválták a jogosultsághalmazát, de a munkavállaló a Google accountjába szinkronizálta a belépési adatait. Oda a NISZ-es hozzáféréshez szükséges autentikációit nyilatkozata szerint nem szinkronizálta fel. A támadóknak a Google irányába nyitva maradt egy session, a jelszót így szerezték meg. Az incidens a cégcsoporti hálózatban történt, nem az éles KRÉTA rendszerben. Az érintett felhasználónak nem volt rendszergazdai jogosultsága. Az Ügyfél a Hatóságnak átadta az incidens bekövetkezését követő IT biztonsági és egyéb intézkedésekről szóló feljegyzést, illetve azt nyilatkozta, hogy a munkavállalók hozzáférési jogosultságairól szóló naplóállományokat átadja a Hatóságnak. 600 kollégájuknak van VPN hozzáférési jogosultsága a covid járvány miatt.

24. Az érintett felhasználó a levelezéshez, belső kommunikációt támogató chatrendszerhez, a KRÉTA rendszer forráskódjait tartalmazó informatikai fejlesztői rendszerhez, support rendszerhez fért

hozzá állandó jelleggel, illetve a support feladatai ellátása kapcsán időlegesen hozzáfért a KRÉTA rendszerben személyes adatokhoz.

25. Az Ügyfél nyilatkozata szerint semmilyen információjuk nem volt arra vonatkozóan, hogy személyes adat került volna ki, a KRÉTA rendszer védett állami környezetben fut. Aki jogosultan lép be, annak nincs további belső szűrése. Nem észlelték, hogy nagy mennyiségű adat áramlott ki a VPN-en keresztül.

26. A 2022 szeptemberében történt incidensnél a VPN-en nem volt nagy adatmozgás, az Ügyfél ezért lezárta az ügyet. Ezt követően, 2022 novemberében jelent meg a belső kommunikációs felületen a támadók arról szóló üzenete, hogy feltörték a rendszerüket. Ekkor szembesült vele az Ügyfél, hogy nagyobb a probléma, mint hitték, és megtették a szükséges bejelentéseket, továbbá megvizsgálták azokat a környezeteket, ahol a fejlesztők dolgoztak. Ebben érintettek voltak olyan excel táblázatok, melyekben voltak az éles KRÉTA rendszerből lementett személyes adatok. Ezek azért voltak az Ügyfélnél, mert az érintett felhasználó support tevékenységet, és különböző, a KRÉTA rendszerrel kapcsolatos hibajavítási munkálatokat végez, valamint megkereséseseket teljesít, melyek elvégzéséhez szükséges lehet az éles rendszerből az adatok átemelése. A megkeresésesek […] rendszeren keresztül vagy e-mailen keresztül érkeznek az Ügyfélhez, magában a hibabejelentő üzenetekben is többször előfordul, hogy személyes adatok szerepelnek. Ezeket a személyes adatokat tartalmazó fájlokat az Ügyfél rendszeresen törli, nem vezet nyilvántartást arról, hogy milyen személyes adatok kerültek így át a rendszerükbe, de ez az éles rendszerben tárolt összes személyes adat kevesebb mint 1%-át teszi ki.

27. A támadó érvényes jogosultságokkal lépett be, ezért a belső tevékenységek logjait az Ügyfél nem tudja követni, nem tudja átadni. *Az Ügyfél nyilatkozata szerint nem lehet kizárni, hogy az érintett felhasználó VPN hozzáférésén keresztül hozzáfértek az éles rendszerhez.* Elvi szinten tehát elképzelhető, hogy VPN-en keresztül bejutottak a NISZ Zrt.-nél kezelt éles rendszerbe, de ennek tényleges bekövetkeztét sem a NISZ Zrt.-nél, sem az Ügyfélnél nem erősítette meg semmilyen vizsgálat.

28. A support tevékenység közben 2022. szeptember 10. és 2022. november 9. napja között az éles rendszerből lementett adatok 10 intézményt érintettek (kb. 1.3 millió személyes adat). A Hatóság kérdésére az Ügyfél azt nyilatkozta, hogy az 1.3 millió személyes adat csak egy becslés, és nincs róla tudomásuk, hogy pontosan kiknek és milyen típusú személyes adatai ezek.

29. Az Ügyfél IT szakértője arról a sajtóban megjelent információról, hogy 238GB adat ki lett másolva a rendszerből, nem tudta megmondani, hogy helytálló-e, ezt a logokból lehetne kideríteni.

30. A szeptemberi incidensről való értesítés az intézményektől jött be, az Ügyfelet kérték fel vizsgálatra, mint adatkezelők kérték az adatfeldolgozó segítségét saját incidensük vonatkozásában, ezért nem látta szükségesnek akkor az Ügyfél a bejelentést.

31. Az Ügyfél korábban próbálta a password policyt megváltoztatni a felhasználók irányába, de ez a Klebelsberg Központ részéről nem nyert támogatást. A novemberi észlelés esetén 2022. november 8. napján belső vizsgálat folyt, feltették a KRÉTA rendszer felhasználói oldalára 2022. november 10. napján a tájékoztatást. Minden intézményvezető részére megjelent egy üzenet, amely megerősíti a támadás tényét, de leírja, hogy az éles rendszerhez nem fértek hozzá. A tájékoztatás szövegét az Ügyfél a Hatóság felé tett adatvédelmi incidensbejelentéshez mellékelte. A support tevékenység közben az Ügyfél belső rendszereibe lementett személyes adatok érintettjeit és adatkezelőit külön nem értesítették az incidenssel kapcsolatban, csak a fenti tájékoztatást közölték velük.

32. Az éles KRÉTA rendszer eléréséhez a kétfaktoros autentikáció beállítására csak november 10. napján került sor.

33. Három modulnak került ki a forráskódja, ami a teljes forráskód 20%-át jelenti. A kikerült forráskód a helyszíni szemle időpontjára már módosult, az egyezés kb. 90 %-os volt. Az Ügyfél nem észlelte a forráskód kimentését.

34. Nem volt arra utaló jel, hogy a támadó a Hatóság által végzett helyszíni szemle időpontjában is hozzáféréssel rendelkezett volna az Ügyfél rendszereihez. A külföldi IP címek letiltásra kerültek, az Ügyfél kollégái azóta is folyamatosan figyelték ezeket a tevékenységeket.

35. A szemle végén az Ügyfél képviselői a helyszínen átadták a Hatóság részére az érintett felhasználó 2022. szeptember 14. napjától 2022. november 8. napjáig terjedő időszakra vonatkozó VPN adatforgalmát, illetve az Ügyfél részéről a következő, a RUFUSZ Zrt. által teljesítendő vállalások történtek:
    - jogosultság mátrix megküldése a Hatóság részére az érintett felhasználó kapcsán 2022. november 22. napjáig,
    - az érintett felhasználó 2022. november 8-17. napja közötti időszakra vonatkozó VPN adatainak megküldése a Hatóság részére,
    - feltehetően releváns szűrt felhasználói logok.

36. 2022. november 30. napján az Ügyfél a Hatóság által korábban írásban feltett kérdésekre megküldte a válaszát, ezek összefoglalva az alábbiak voltak.

37. A KRÉTA rendszer vonatkozásában az Ügyfél kizárólag adatfeldolgozói szerepkört tölt be, adatkezelőknek az alábbi köznevelési intézmények (iskolák) tekintendők:
    - szülő / gyermek felhasználók esetén az az intézmény, melynek a gyermek a tanulója
    - pedagógus / egyéb foglalkoztatott személy esetén az őket foglalkoztató intézmény.

38. A köznevelési intézmények gyűjtik az érintettektől a személyes adatokat, és ők határozzák meg a tanulókról / gondviselőkről / alkalmazottakról nyilvántartott adatok kezelésének célját, módját és eszközeit a nemzeti köznevelésről szóló 2011. évi CXC. törvény vonatkozó rendelkezései alapján. Az Ügyfél a KRÉTA rendszer vonatkozásában adatfeldolgozónak tekintendő, a KRÉTA rendszert használó intézményekkel vagy fenntartóikkal megkötött KRÉTA rendszerre vonatkozó Szoftvertermék szolgáltatási szerződés (vagy vállalkozási szerződés) és hozzájuk kapcsolódó adatfeldolgozási szerződés alapján.

39. Az Ügyfél a szerződések alapján ellátja a KRÉTA terméktámogatási szolgáltatásokat, melyek az alábbiakat tartalmazzák:
    - Ügyfélszolgálat – Helpdesk működtetése
    - Rendszerkövetés, jogszabálykövetés elvégzése
    - Bejelentés kezelés (KRÉTA Rendszer bejelentett hibáira vonatkozóan a bejelentést követően megkezdi a hibák elhárítását)
    - Szoftverfrissítés elvégzése
    - Szakértői, tanácsadói tevékenység
    - KIR interface támogatás
    - Oktatás megtartása
    - KRÉTA információbiztonsági és adatvédelmi audit támogatása
    - Havi eredménytermékek elkészítése (KRÉTA terméktámogatásról szóló jelentés; KRÉTA Szoftverfrissítésről szóló jelentés; KRÉTA Terméktámogatás (bejelentések) jelentése az érintett modulok vonatkozásában)

Az Ügyfél biztosítja továbbá a szerződés alapján a hatóságok, intézmények részére az adatszolgáltatások elvégzését is.

40. Az Ügyfél álláspontja szerint a határozat elején linkelt cikkekben foglaltak nem tartalmazzák teljes egészében a valós eseményeket. Az adathalász támadás a lefolytatott vizsgálataik szerint nem az éles KRÉTA rendszert, kizárólag az Ügyfél belső munkavégzésre és munkaszervezésre használt eszközeit érintette. 2022. szeptember 15. napján több intézménytől érkezett megkeresés az Ügyfél felé, hogy az intézmények alkalmazottjai kártékony kódot tartalmazó linkkel ellátott üzenetet kaptak a KRÉTA rendszeren keresztül. A kártékony kódot kivizsgálás céljából Outlook levelező rendszeren keresztül küldték át az Ügyfélnek az ügy kivizsgálásban érintett kollégáinak. Ekkor kattintott az érintett felhasználó a linkre annak megvizsgálása céljából. 2022. szeptember 18. napján (vasárnap) az érintett felhasználó a Gmail fiókján keresztül kapott értesítést gyanús tevékenységről (belépésről), és ekkor jelszót változtatott. A […] bérszámfejtő programtól is érkezett a munkahelyi e-mail címre levele, hogy kétfaktoros autentikációhoz tartozó kóddal erősítse meg a belépését. 2022. szeptember 19. napján jelezte az érintett felhasználó a problémát a felettesének és az üzemeltetési csoportvezetőnek, és beszámolt egyúttal arról is, hogy korábban rákattintott a kártékony kódot tartalmazó linkre. Az Ügyfél üzemeltetéssel foglalkozó kollégái – miután izolált környezetben lefuttatták a kártékony kódot tartalmazó linket – felszólították a munkavállalókat 2022. szeptember 21. napján 15:20 perckor, hogy haladéktalanul vizsgálják át a számítógépeiket, és ellenőrizzék, hogy egy adott mappa települt-e a számítógépükre. Az érintett felhasználó a nevezett mappát megtalálta a számítógépén, más munkavállaló esetén ez a mappa nem települt a számítógépre. Az eset észlelésével párhuzamosan az Ügyfél vezérigazgatóját is tájékoztatták az eseményekről és a javasolt, azonnali intézkedésekről. Az érintett felhasználó belépési azonosítói, jogosultságai 2022. szeptember 21. napján 16:00 körül, a mappa észlelése után haladéktalanul inaktiválásra kerültek, a gépe levételre került a hálózatról. Szintén aznap az érintett felhasználó bevitte a számítógépét a Rufusz Computer Informatikai Zrt.-hez, új számítógépet kapott, és új jelszót is. Ezt követően fokozatosan kapta vissza a VPN és egyéb jelszavakat. 2022. szeptember 22. napján a kapott új számítógépet és jelszót az érintett felhasználó üzembe helyezte az Ügyfél hálózatán (mivel az első belépéshez belső hálózati csatlakozás szükséges). Az üzemeltetési csoportvezető irányításával az összes korábban használatban levő jelszavát megváltoztatta. Az Ügyfél kijelölt kollégái kivizsgálták az egyes bejelentéseket, elemezték a belépéshez tartozó log adatokat, annak érdekében, hogy a szükséges intézkedéseket megtegyék. 2023. szeptember 23. napján az összes éles környezet bejövő forgalmán korlátozásra kerültek a külföldi IP címekről érkező kérések, továbbá felkérésre került a NISZ Zrt. is, hogy intézkedjen a külföldi IP címek kitiltásáról. 2022. szeptember 23. napján az Ügyfél felvette a kapcsolatot a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettel, az általuk javasolt lépéseket (jelszóváltoztatás, gépek átvizsgálása) megtette.

41. Mivel a támadó az Ügyfél munkavállalójának felhasználónevével és jelszavaival – bármely módosítás és aktivitás nélkül – tartózkodott bent a belső rendszerekben, a támadás változatlan fennállásáról és az incidens bekövetkezésének lehetőségéről csak 2022. november 7. napján szerzett az Ügyfél tudomást, amikor a belső kommunikációs felületen a támadó arról szóló üzenete jelent meg, hogy feltörhették az Ügyfél belső rendszereit. A tudomásszerzést követően még aznap kérte az Ügyfél szakértők közreműködését arra vonatkozóan, hogy mely rendszereket érintette / érinthette a támadás. A részletes vizsgálat lefolytatása hosszabb időt vett igénybe. A vizsgálat menetéről és annak eredményéről szóló jegyzőkönyv megküldésre került a Hatóság részére. A vizsgálatokat követően 2022. november 10. napján az Ügyfél megkezdte az adatvédelmi incidens Hatóságnak történő bejelentését.

42. Az Ügyfél álláspontja szerint az adatvédelmi incidenst a támadónak az Ügyfél belső rendszereihez, az azokon szereplő adatokhoz való jogosulatlan hozzáférése idézte elő. Az incidenshez kapcsolódó kockázatértékelés szintén megküldésre került a Hatóság részére. A

vonatkozó naplófájlok egy részét az Ügyfél a Hatóság által lefolytatott helyszíni szemle során a Hatóság munkatársainak átadta, a további log adatokat és vonatkozó jogosultságokat pedig a válaszlevél mellékleteként juttatta el a Hatóságnak.

43. Az Ügyfél a szoftvertermék támogatására vonatkozó szerződés alapján kialakított kommunikációs protokollnak megfelelően az adatkezelőket az alábbi (intézmények KRÉTA fiókjainak főképernyőjén elhelyezett) rendszerüzenettel értesítette 2022. november 10. napján: *„Tisztelt Címzettek! Az eKRÉTA Informatikai Zrt. az internetes hírportálokon közzétett cikkekben foglaltakkal összefüggésben a Társaság belső fejlesztői környezeteit, munkaszervezésre és munkavégzésre használt belső csatornáit érintő támadással kapcsolatban az incidens gyanúját a jogszabályoknak megfelelően jelentette a Nemzeti Adatvédelmi és Információszabadság Hatóságnak. Társaságunk jelenleg is vizsgálatot folytat az esetlegesen érintett rendszerek, adatok feltárására vonatkozóan.”*

44. A Hatóság 2022. december 19. napján kelt, NAIH-8516-10/2022 iktatószámú levelében feltett kérdéseire az Ügyfél az alábbi válaszokkal szolgált.

45. A KRÉTA rendszerből korábban lementett személyes adatokat (melyek tesztelés céljából az érintett felhasználó számítógépén a támadás időpontjában éppen elérhetőek voltak), az érintettek számát és az adatok mennyiségére vonatkozó információkat a válaszhoz mellékletként megküldött excel táblázat tartalmazta, melyben 12 darab szakképzési centrumhoz kapcsolódóan szerepelnek (a jelen határozat 59-60. bekezdésében szereplő) személyes adatok, összesen – az excel táblázatban szereplő adatok szerint - 8574 tanuló ~290.000 adata, 11.082 gondviselő ~44.000 adata, valamint 1205 alkalmazott ~35.000 adata.

46. Az Ügyfél belső rendszerei tekintetében az érintettek az Ügyfél azon munkavállalói, akik az érintett belső kommunikációs rendszerhez hozzáférnek. A munkavállalóknak kizárólag a neve (teljes neve vagy kitalált felhasználóneve), mellyel a belső üzenetküldő rendszerbe bejelentkezik, vált illetéktelenek számára elérhetővé. A további belső rendszerekben esetlegesen elérhetővé vált személyes adatok mennyiségéről és kategóriáiról az Ügyfél a Hatóság kérdésére 2023. december 8. napján adott választ, a következők szerint. 2022 novemberében az Ügyfélnek 138 fő alkalmazottja volt, ebből 36 fő tartozott a KRÉTA Projektigazgatósághoz, mint szervezeti egységhez, ahova munkaköre alapján az érintett felhasználó is. Az érintett felhasználó a következő rendszerekbe volt bejelentkezve a támadás időpontjában: […], […], […] (jelszavak tárolása), Notepad++, VPN, Total Commander, Office 365 és Outlook, Slack (belső kommunikációs platform), webböngészők, ügyvitel, […] (szabadságnyilvántartó alkalmazás). A belépés a Slack és a […] kivételével mindenhova a céges fiókba történő belépéshez használt autentikációval […] lehetséges, a Slack alkalmazásba munkahelyi e-mail címmel és saját jelszóval, a […]-be pedig felhasználónévvel és jelszóval lehet belépni. A Slack üzenetküldő rendszeren a kollégák egymás nevét, mint személyes adatot láthatják, így a támadó ezen a felületen a belépett munkavállalók neveit láthatta. A munkavállalók ezen a platformon néha (munkahelyi kötődésű) személyes fényképeket is megosztanak egymással, ennek következtében a támadó az egyik kollégáról készült képet letöltötte az üzenetküldő rendszerből, és közzétette a Telegram csatornán (ahol a KRÉTA forráskódját is publikálta). Az Outlook levelező rendszert az Ügyfél minden munkavállalója használja, abban megtalálható a munkavállalók neve, beosztása, elérhetősége (e-mail cím, telefonszám). A támadó számára azon levelezések adatai válhattak megismerhetővé, akivel az érintett felhasználó az azt megelőző időszakban levelezést folytatott. A […] rendszerben szintén látható a munkavállalók neve, és az, hogy a munkavállaló szabadságon van. A […] esetén a KRÉTA rendszerből származó anonimizálatlan tesztadatokhoz férhetett hozzá a támadó (ld. 45. bekezdés). Az Ügyfél megemlítette, hogy az incidens kivizsgálása során a belső rendszerek vizsgálatát megelőzően a hangsúlyt elsődlegesen a KRÉTA rendszert ért esetleges incidens vizsgálata előzte meg, melynek eredményeképpen megállapítást nyert, hogy a KRÉTA

rendszert nem érte adathalász támadás. Egy külső állami tulajdonú vállalkozó 2023 december végéig vizsgálatot folytat az Ügyfél részére, melynek keretében a KRÉTA rendszer felhasználóira vonatkozó adatok felderítését célzó keresést folytat az ún. dark weben[1].

47. A tényállás megfelelő tisztázása érdekében a Hatóság a NISZ Zrt.-t is megkereste több alkalommal, a NISZ Zrt. válaszaiból az alábbiak derültek ki.

48. A NISZ Zrt. a KRÉTA rendszer vonatkozásában kizárólag bizonyos infrastruktúra (IaaS) és tűzfal szolgáltatásokat biztosít a Klebelsberg Központ, mint megrendelő számára, a KRÉTA alatt futó operációs rendszerek, illetve a KRÉTA alkalmazás üzemeltetése kívül esik ezen szolgáltatási körön. A tűzfalon a KRÉTA rendszerre vonatkozóan a NISZ Zrt. kizárólag az Ügyfél kérése alapján végez beállításokat, tekintettel arra, hogy az ún. OSI-modell szerinti szállítási rétegig (layer 4 szintig) nyújt szolgáltatást. Ennek keretében a NISZ Zrt. tevékenysége a következőkre terjed ki: IP-cím és port engedélyezése vagy tiltása a forrás és a cél között.

49. A fentiek alapján a NISZ Zrt.-nek sem az alkalmazáshoz vagy adatokhoz való hozzáférésekről, sem azok jogos vagy illetéktelen voltáról nem áll módjában nyilatkozni, mert ezek a tevékenységek alkalmazásszinten (alkalmazás rétegben, layer 7 szinten) történnek. A NISZ Zrt. a nyújtott szolgáltatások körében a hálózati (layer 3-4) szint fölötti eseményeket nem figyeli és nem naplózza.

50. A NISZ Zrt.-t nem kereste meg az eKRÉTA Zrt. a náluk bekövetkezett adatvédelmi incidenssel összefüggésben, erről a NISZ Zrt. a sajtóból értesült. A Klebersberg Központ 2022.09.22-én 14:43-kor feladott e-mailben kérte a NISZ Ügyfélszolgálaton a „*KRÉTA rendszer külföldi elérésének ideiglenes blokkolását*”. E kérés indoklása a következő volt: "*Az elmúlt napokban sajnálatos módon megnövekedett a KRÉTA rendszer elleni támadások száma. A támadások különféle módszerekkel történnek, de közös jellemzőjük, hogy a próbálkozások szinte kizárólag külföldi IP címekről történnek*."

51. Kiegészítésként a NISZ Zrt. az alábbi kérést kapta 2022. szeptember 26. napján az Ügyféltől: „Kérem vizsgálják felül az eszközölt beállításokat, ugyanis 2022-09-24 10:21:25.727-kor például a […] IP címről még történt sikeres próbálkozás!”

52. A NISZ Zrt.-nek nincs tudomása arról, hogy az éles rendszert érintő, fenti tűzfalbeállítási kérések a sajtóban megjelent adatvédelmi incidenssel összefüggésben állnak-e.

53. A NISZ Zrt. érintett határvédelmi rendszere (tűzfal) felhasználói azonosítást (autentikáció) és hitelesítést (authorizáció) nem végez, így a hozzáférések illetéktelenséget nem tudja vizsgálni. A NISZ Zrt. az illetéktelen hozzáféréssel kapcsolatban vizsgálatot saját hatáskörben nem folytatott.

54. A NISZ Zrt. a KRÉTA rendszerrel kapcsolatos üzemeltetési szolgáltatásainak szintje (IaaS) miatt nem illetékes azon kérdés megválaszolásában, miszerint kizárható-e teljes mértékben, hogy az éles KRÉTA rendszerhez a támadó(k) hozzáférést szereztek, onnan adatokat mentettek le.

[1] A dark web egy olyan része az internetnek, amely elrejtve marad a hagyományos keresőmotorok számára, ez a mély web (deep web) egy speciális része, ahol az anonimitásnak és a titkosításnak kiemelt szerepe van. Az itt zajló tevékenységek között lehetnek törvényes és jogosult célú kommunikációk is, de gyakran előfordulnak illegális tevékenységek, például drogkereskedelem, fegyverkereskedelem, kibertámadásokra készülés, és egyéb illegális szolgáltatások. Azért is nevezik "sötét" webnek, mert az elrejtettsége és az anonim mivolta miatt nehezen nyomon követhető.

55. Az Ügyfél a Hatósághoz 2023. március 8. napján érkezett levelében az alábbi tájékoztatást adta.

56. Az Ügyfél egy […] VPN kapcsolaton keresztül férhet hozzá a NISZ Zrt.-nél levő éles KRÉTA rendszerhez a felépülő VPN tunnel-ben (ami egy titkosított kapcsolat az eszköz és a VPN kiszolgáló között). Ez titkosítási kulcs nélkül feltörhetetlen, így sem a támadók, sem internetszolgáltató (ISP) nem férhet hozzá az adatokhoz. A VPN tunnel gyakorlatilag egy privát útvonalat jelent az internethez közvetítő szerveken keresztül, nincs protokoll vagy port szintű korlátozás. A fogadó oldalon a VPN kapcsolat felépítése kizárólag titkosított SSL csatornán történik. A VPN egy szabványos […] VPN. Az Ügyfél forráscíme: […]. Az éles KRÉTA rendszer cél IP címei: […] és […].

57. Az Ügyfél fejlesztői környezetéhez használt VPN rendszerben is letiltásra kerültek a külföldi IP címtartományok 2022. november 9-ei dátummal.

58. A rendelkezésre álló naplóállományokból csak azt tudják megállapítani, hogy az érintett felhasználó azonosítójával és jelszavával, kizárólag az Ügyfél szokásosan használt rendszerein keresztül léptek be az éles KRÉTA rendszerhez, utólag nem lehet megállapítani, hogy volt-e ezek között illetéktelen bejelentkezés.

59. Felhasználói szintű hozzáféréssel az Ügyfél nem rendelkezik a KRÉTA rendszerhez, de a KRÉTA rendszer mögött futó adatbázisokhoz, logolási rendszerekhez, alkalmazás szerverekhez az Ügyfél VPN kapcsolaton keresztül az együttműködési megállapodásban részletezett feladatok ellátása érdekében - kizárólag nevesített felhasználókkal, szükséges és elégséges jogosultságokkal - hozzáfér. **Ezáltal az Ügyfél a KRÉTA rendszerben tárolt jelszavakon kívül minden, a KRÉTA rendszerben tárolt adathoz hozzáfér, melyek:**

Alkalmazottra (pedagógus, iskola titkár) vonatkozó adatelemek	Kötelezően kitöltendő/nem kötelező
neme	Igen
szül.dáum	Igen
szül.név	Igen
anya neve	Igen
állampolgárság	Igen
szül.ország	Igen
név	Igen
anyanyelve	Igen
Oktatási azonosító	Igen
adóazonosító jel	Nem
TAJ szám	Nem
főállású-e	Igen
szakértői/viszgaelnőki tevékenységet végez-e	Igen
rendelkezik szakvizsgával	Igen
rendelkezik e továbbképzéssel	Igen
kezelheti-e a diákok közösségi szolgálatait	Igen
alkalmazás kezdete/vége	Igen
kötelező óraszám	Igen
munkakör típusa	Igen
munkaviszony típusa	Igen
tartós helyettesítésre lett-e felvéve	Igen
tartós helyettése van-e	Igen
besorolási fokozata	Igen
munkaidőkedvezmény oka	Igen
nyugdíjas-e	Nem
foglalkoztatás típusa	Igen
vezetői órakedvezmény oka	Igen
áttanító-e	Nem
pedagógus végzettségei	Nem

60.

Gondviselőre vonatkozó adatelemek	Kötelezően kitöltendő/nem kötelező
név	Igen
rokonság foka	Igen
elérhetőségi adatok (lakcím, tel.szám, email)	Nem
törvényes képv-e	Igen

ADATKÖRÖK

Tanulóra vonatkozó adatelemek	Kötelezően kitöltendő/nem kötelező
neme	Igen
szül.dátum	Igen
szül.név	Igen
anya neve	Igen
állampolgár	Igen
szül.ország	Igen
név	Igen
anyanyelve	Igen
Oktatási azonosító	Igen
adóazonosító jel	Csak Szakképzésben kötelező
TAJ szám	Csak Szakképzésben kötelező
bankszámlaszám	Csak Szakképzésben kötelező
BTMN (beilleszkedési, tanulási, magt, nevelési nehézséggel rendelkező)	Igen
SNI(sajátos nevelési igényű)	Igen
Diákig.szám	Nem
Államilag gondozott-e	Igen
évismétlő-e	Igen
ingyentankönyv jogosult	Igen
jogviszony adatok	Igen
sajátos munkarendben tanul-e	Igen
részedül-e szoc támogatásban	Igen
tandíjköteles-e	Igen
tankötelezett-e	Igen
vendégtanuló-e	Igen
kollégiumi ellátásban részedsül-e	Igen
rendszeres gyermekvédelmi kezdvezmény	Igen
sportjellemzők	Nem
vallása	Nem
szakképzéssel kapcsolatos adatok (szakmai ágazatra vonatkozó adatok)	Csak Szakképzésben kötelező
osztálybesorolásai	Igen
tanuló mulasztás adatai	Igen
tanuló értékelései	Igen
tanuló kapott feljegyzései	Igen
elérhetőségi adatok (lakcím, tel.szám, email)	Igen

61. **Az éles KRÉTA rendszerben az Ügyfél tájékoztatása szerint összesen kb. 225 ezer alkalmazott, másfélmillió diák és 1.87 millió gondviselő személyes adata található meg. Ez a személyes adatok mennyiségét illetően az alkalmazottak esetében ~6.5 millió, diákok esetében ~47 millió, gondviselők esetében pedig ~7.5 millió adatot jelent** (az adatok töltöttsége folyamatosan változik a felhasználók és az intézmények adattöltési szokásai és a be- és kiiratkozások alapján). A KRÉTA rendszerben megjelenő adatkörökhoz a felhasználók nem minden esetben rögzítenek adatot, amennyiben az adott mező kitöltése nem kötelező.

✧✧✧

62. A Hatóság az eljárás során alaposan vizsgálta, hogy az 51. bekezdésben említett IP cím összefüggésbe hozható-e az ügy tárgyát képező esettel. Ennek során a NISZ Zrt. a Hatósághoz 2023. május 16. napján érkezett levelének mellékleteként megküldött a Hatóság részére egy olyan táblázatot, mely a Hatóság által jelzett vizsgálati időszakra (2022. szeptember 15. – 2022. november 7.) vonatkozóan azokat a szűrt logsorokat tartalmazta, amelyek esetében a forrás IP cím az 51. bekezdésben említett […]. A NISZ Zrt. a rendelkezésre álló forgalmi adatok alapján nem tudta megállapítani, hogy az éles KRÉTA rendszer szerverhez milyen hozzáférés történt. Az üzemeltetési feladatok ellátása és végrehajtása egy, kizárólag ezen feladatok ellátására kialakított és fenntartott, védett csatornán keresztül történő távoli hozzáféréssel történik, erre vonatkozóan szabálymódosítás a vizsgált időszakban nem történt.

63. Ezzel kapcsolatban a Hatóság informatikai szakértői 2023. június 5. napján informatikai szakértői véleményt készítettek, mely – többek között - az alábbi megállapításokat tartalmazta:

64. A KRÉTA rendszer feltörésével kapcsolatosan a Hatóság NISZ Zrt.–nek feltett kérdéseire 2023. május 16. napján beérkezett válaszok, illetve bizonyítékként megküldött naplófájlok alapján megállapítható, hogy a logok nem teljesek. A NISZ Zrt. technikai hibára hivatkozik és ezért a log-ok egy jó része hiányzik. A kérdések többek között a NISZ Zrt. korábbi, az Ügyféllel folytatott levelezésében említett támadó IP címre is vonatkoztak, amely esetben biztosan tudjuk (az Ügyfél NISZ-nek küldött e-mailje alapján), hogy illetéktelen behatolás történt arról az IP címről. Az említett „támadó” IP cím: […]

65. […]

66. A NISZ Zrt.-től kapott log-ok a levelezésben megjelölt napot ugyan tartalmazták, bár ez a naplófájl sem volt teljes. A naplófájlokból a Hatóság informatikai szakértői kiolvasták, hogy a támadó IP címen keresztül két másik IP címet értek el a „támadók”: […] és […].

67. Az Ügyfél által az e-mailben közölt időpontban a […] IP címet érték el a támadó IP címről. Mindkét IP címet a log-ból is láthatóan a 443–as porton, vagyis HTTPS protokollon keresztül érték el. Ezt az IANA által szabványként megállapított és széles körben szabványosan használt portot az ún. SSL-tanúsítvánnyal megvalósított, a kliens és szerver közötti titkosított kommunikációhoz használják az informatikában. Éles adatokat tartalmazó teszt rendszert nem szokás kitenni publikus hálózatra, ez nem felel meg a legjobb iparági gyakorlatnak, zárt/védett belső hálózaton üzemelnek az ilyen jellegű teszt rendszerek, a távoli elérés pedig védett csatornán biztosítandó. A fent említett IP címeket megvizsgálva az látszik, hogy a támadók az éles rendszerhez is hozzáférhettek. A […] végű IP cím az internetről elérhető éles KRÉTA rendszerhez tartozik. Mind a két IP cím, amit elért a támadó, az éles KRÉTA rendszer autentikációs felületére vezet, ahol a belépési adatok megadása után az elektronikus ügyintézést tudják a felhasználók indítani.

68. Az informatikai szakértői vélemény tájékoztatás céljából megküldésre került az Ügyfélnek is, aki az abban foglaltakra az alábbiakban reagált.

69. Az Ügyfélhez 2022 szeptemberében a rendőrségtől több megkeresés is érkezett, miszerint közveszéllyel fenyegetés bűntette miatt nyomozás indult ismeretlen tettes ellen. Az elkövető(k) a KRÉTA rendszer egyes felhasználóinak fiókjába léptek be a felhasználó érvényes adataival, majd kártékony kódot tartalmazó üzenet kiküldésére került sor, mely linkre több felhasználó rákattintott. Az Ügyfél az intézmények és a rendőrség kérésre ekkor kivizsgálta az akkori eseményeket, és a vizsgálat során megállapította, hogy az illetéktelennek vélt bejelentkezések többségében külföldi IP címekről történtek. Emiatt az Ügyfél munkatársai a további támadások megakadályozása

érdekében intézkedtek a külföldi IP címek letiltásáról. Ezen beállításról a NISZ Zrt. kollégáit is értesítették, és kezdeményezték, hogy a NISZ Zrt. is tegye meg a szükséges intézkedéseket a külföldi IP címek letiltására. Az […] IP cím esetében az Ügyfél munkatársai ismét észleltek belépést, illetve belépési próbálkozásokat, ezért kérték újra a NISZ Zrt.-től a külföldi IP címekre vonatkozó beállítások ellenőrzését.

70. Az 51. bekezdésben említett levéllel kapcsolatban az Ügyfél megjegyezte, hogy ezen esetben illetéktelen jelszóhasználat történt, azaz a „támadó" megszerezte a felhasználó felhasználónevét és érvényes jelszavát, ezzel lépett be. A szakértői véleményben szereplő IP címek a KRÉTA rendszer publikus IP címei […], melyeket bárki elérhet és érvényes felhasználónévvel, valamint érvényes jelszóval be tud lépni az adott KRÉTA rendszerbe. A fenti két IP cím esetében helyes a szakértő megállapítása, miszerint „*a fent említett IP-ket megvizsgálva az látszik, hogy a támadók az éles rendszerhez is hozzáférhettek"*.

71. Minden felhasználó ezeken az IP címeken keresztül lép be a KRÉTA rendszerekbe érvényes felhasználónév és jelszó birtokában. Az Ügyfél hangsúlyozta, hogy ezek az IP címek, és az 51. bekezdésben említett levél is az éles publikus KRÉTA rendszerre vonatkoznak.

72. Egyetértett továbbá az Ügyfél a szakértői vélemény azon megállapításával is, miszerint „*mind a két IP cím, amit elért a támadó, az éles Kréta rendszer autentikációs felületére vezet, ahol a belépési adatok megadása után az elektronikus ügyintézést tudják a felhasználók indítani*".

73. **A fentiek alapján a Hatóságnak az eljárás során nem sikerült kétséget kizáróan összefüggést teremtenie a […] IP címről folytatott támadás és az ügy tárgyát képező adatvédelmi incidens, illetve az azt okozó támadás között, így az eljárás során ebben a tekintetben feltárt körülmények a szankciók kiszabása során nem kerültek figyelembevételre.**

✧✧✧

74. Az Ügyfél 2023. október 30. napján küldött válasza értelmében az általa folytatott naplózással kapcsolatban előadta, hogy a KRÉTA rendszerben nem szerepkörök szerinti, hanem alkalmazás szintű logolás történik. Az egyes naplóbejegyzések az alábbi események esetén rögzítik a következő adatokat: 1) rekord (vagyis adott eseményhez tartozó naplóbejegyzés) létrehozása (ki és mikor hozta létre az adott rekordot), 2) rekord módosítása (ki és mikor módosította a rekordot, az eredeti és a módosított érték is tárolásra kerül), 3) rekord törlése (ki és mikor törölte a rekordot).

75. Az Ügyfél alkalmazottjai a következő hozzáféréssel rendelkeznek a naplóbejegyzésekhez: 1) üzemeltetés / ITB felelős (hozzáférés szintje: teljes), 2) terméktámogatás (hozzáférés szintje: olvasási jog), 3) fejlesztők (hozzáférés szintje: olvasási jog), 4) fejlesztők CI/CD[2] eszközök használatakor (telepítés) (hozzáférés szintje: teljes, telepítés/módosítás során).

76. A Hatóság kérdésére az Ügyfél szintén tájékoztatta a Hatóságot azokról az intézkedésekről, amelyeket az incidens következtében foganatosított. Ezek az alábbiak voltak:

[2] A **CI/CD** olyan módszertan a szoftverfejlesztésben, amely a folyamatos integrációt (Continuous Integration: CI) és a folyamatos szállítást (Continuous Delivery: CD) egyesíti.
A folyamatos integráció olyan fejlesztési gyakorlat, amelyben a fejlesztők a kódot naponta többször egy közös felületen integrálják, egyeztetik, így a kisebb változtatások is gyorsan elérhetővé válnak a csapat többi tagja számára. Az integrálást követően minden új kódrészlet ellenőrzésre kerül, amely lehetővé teszi a fejlesztők számára, hogy korán felismerjék a problémákat és még az elején javítsák azokat, így időt nyerve és minimalizálva a javítandó kódok mennyiségét.
A folyamatos szállítás célja, hogy minél előbb visszajelzés érkezzen a munkáról, hogy azt minél jobban a megrendelő igényeihez lehessen igazítani.

a) Hitelesítési megoldások felülvizsgálata, szabályozás áttekintése: 2022 november-decemberében megtörtént.
b) E-mail biztonság felülvizsgálata: Az adathalász tevékenységről a KRÉTA központi oldalán elhelyezésre került egy tájékoztató, illetve az Ügyfél munkavállalói külön, a belső rendszerekre és saját e-mailekre vonatkozó tájékoztatást kaptak ebben a témakörben. Egy „Böngésző biztonságos jelszó tárolása" című dokumentum, illetve egy adathalász levelek felismerésére szolgáló általános tájékoztató kiküldésre került szintén a munkavállalók számára.
c) A külföldi IP címek letiltásra kerültek a KRÉTA rendszerek WEB elérhetőségein, valamint az Ügyfél VPN elérhetőségein (egyedi bejelentés alapján kivételi listák engedélyezhetőek).
d) Az Ügyfél belső hálózatához tartozó felhasználónevek és jelszavak biztonságának fokozása érdekében utasítás került kiadásra 2022 novemberében. Ez tartalmazza, hogy tilos elmenteni a céges rendszerek (Outlook, […], […], PROD vagy UAT környezeten lévő KRÉTA, illetve egyéb KRÉTA modul, stb.) felhasználóihoz tartozó jelszavakat a böngészőben. A nem AD autentikációt használó rendszerekhez eltérő jelszavakat kell használni. Az AD policy-t meghaladó, nem kitalálható jelszavakat kell használni. Jelszó megosztása bárkivel tilos. A magán és céges jelszavakat szigorúan szét kell választani.
e) Kétfaktoros azonosítás bevezetése 2022. november 15. napján: Klebersberg Központ VPN elérésére, az Ügyfél belső kommunikációjára használt Slack alkalmazás, és az […] esetében. Az Ügyfél a munkatársaknak a belső rendszerekhez való hozzáférései esetében bevezette a kötelező kétfaktoros azonosítást, valamint megtiltotta saját Google fiók magáncélú használatát a munkahelyi eszközökön.
f) 2023. június 9. napján az Ügyfél új, felülvizsgált és a nemzetközi jó gyakorlatok alapján átalakított IT biztonsági szabályzata közzétételre került.
g) A hálózati erőforrások átalakítása 2023 februárjában megtörtént.
h) Az Ügyfél munkatársai 2023 januárjában adatbiztonsági és adatvédelmi oktatáson estek át.
i) Az adatbázisok oszlop szintű titkosításának lehetősége felmérésre került, azonban a rendszer teljesítményének romlására tekintettel ennek megvalósítása jelenleg nem lehetséges.
j) Minden 2023. október 31. napja után keletkező eseti mentés (copyonly) vagy mentési lánc állományai titkosított formában kerülnek tárolásra. Azok visszaállítása csak a titkosító kulcs birtokában lehetséges.
k) Több faktoros autentikáció bevezetése: az „Új jelszókezelési eljárásrend kialakítása" című dokumentum elkészült, és a funkció fejlesztés alatt áll. Ennek célja a diákok / tanárok /intézményi adminisztrátorok / központi KRÉTA felhasználók és gondviselők regisztrációs és belépési folyamatában a biztonság növelése. A funkció a központi KRÉTA felhasználók/ tanárok /intézményi adminisztrátorok számára bevezetésre került 2023 júniusában.
l) Az Ügyfél adatbázis biztonsági szabályzata (jogosultságkezelés, minimum jogosultság elve, szerepkörök szétválasztása) elkészült, kihirdetése a válasz időpontjában folyamatban volt.
m) A legmagasabb szintű jogosultsági körök az Ügyfél hálózatában 2023 januárjával felülvizsgálatra kerültek.
n) Az NSZFH (Nemzeti Szakképzési és Felnőttképzési Hivatal) környezetében található intézményi KRÉTA SQL szerverének ellenőrzése megtörtént.
o) Minden munkavállaló számára orientáció 2023. október 26. napján, hogy csak Windows vagy tanúsítvány alapú hitelesítést használjanak.
p) Felmérésre került, hogy a kulcsok tárolásához milyen szoftveres és hardveres feltételek szükségesek, ennek a bevezetése a tervek szerint 2023 év végéig megtörténik.
q) A rendszeres API kulcs cserékhez képest időközi kulcscseréket hajtott végre az Ügyfél.
r) Automatizált folyamatokhoz szükséges nem megszemélyesített felhasználók jelszócseréje rendszer szinten:
   A KRÉTA rendszerben alapvetően három ilyen entitás létezik:
   1. […]

2. […]
3. […]

Mindháromnak a cseréje megtörtént 2022 november 7. és 15. napja között.

s) A fejlesztői környezetben használt kódok biztonsági felülvizsgálata megtörtént. Beállításra kerültek olyan peremfeltételek, melyek segítségével az automatizált felülvizsgálat folyamatosan történik. A fejlesztők már csak nevesített felhasználóként tudnak belépni. Az összes projekt esetében folyamatos a felülvizsgálat és a megfelelő kapcsolódási mód beállítása, ahol az szükséges.

II. Alkalmazott jogszabályi rendelkezések

77. Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) 99. §-a alapján a hatóság – a hatáskörének keretei között – ellenőrzi a jogszabályban foglalt rendelkezések betartását, valamint a végrehajtható döntésben foglaltak teljesítését.

78. Az általános adatvédelmi rendelet 2. cikk (1) bekezdése alapján az adatvédelmi incidenssel érintett adatkezelésre az általános adatvédelmi rendeletet kell alkalmazni.

79. Az általános adatvédelmi rendelet 4. cikk 12. pontja határozza meg, hogy mi minősül adatvédelmi incidensnek, ez alapján „adatvédelmi incidens”: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

80. Az általános adatvédelmi rendelet (75) és (76) Preambulum bekezdése értelmében a természetes személyek jogait és szabadságait érintő – változó valószínűségű és súlyosságú – kockázatok származhatnak a személyes adatok kezeléséből, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek, különösen, ha az adatkezelésből hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, a jó hírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, az álnevesítés engedély nélkül történő feloldása, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrány fakadhat; vagy ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett; vagy ha olyan személyes adatok kezelése történik, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utalnak, valamint ha a kezelt adatok genetikai adatok, egészségügyi adatok vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkoznak; vagy ha személyes jellemzők értékelésére, így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából; vagy ha kiszolgáltatott személyek – különösen, ha gyermekek – személyes adatainak a kezelésére kerül sor; vagy ha az adatkezelés nagy mennyiségű személyes adat alapján zajlik, és nagyszámú érintettre terjed ki. Az érintett jogait és szabadságait érintő kockázat valószínűségét és súlyosságát az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében kell meghatározni.

81. Az általános adatvédelmi rendelet 32. cikk (1) bekezdése értelmében az adatkezelő és az adatfeldolgozó a tudomány és a technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatok figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat

mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, (a b) pont szerint) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét.

82. Az általános adatvédelmi rendelet 32. cikk (2) bekezdése értelmében a biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

83. Az általános adatvédelmi rendelet 33. cikk (1) és (2) bekezdése szerint az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is. Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

84. Az általános adatvédelmi rendelet 34. cikk (1) bekezdése alapján, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

85. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 2. § (2) bekezdése szerint az általános adatvédelmi rendeletet az ott megjelölt rendelkezésekben foglalt kiegészítésekkel kell alkalmazni.

86. Az Ákr. 101. § (1) bekezdés a) pontja alapján, ha a hatóság a hatósági ellenőrzés során jogsértést tapasztal, megindítja a hatósági eljárását. Az Infotv. 38. § (3) bekezdése és 60. § (1) bekezdése alapján a Hatóság az Infotv. 38. § (2) és (2a) bekezdés szerinti feladatkörében a személyes adatok védelméhez való jog érvényesítése érdekében hivatalból adatvédelmi hatósági eljárást folytat.

87. Az Infotv. 60. § (3) bekezdés b) pontja értelmében, a Hatóság hivatalból adatvédelmi hatósági eljárást indít, ha vizsgálata alapján megállapítja, hogy a személyes adatok kezelésével kapcsolatban jogsérelem következett be vagy annak közvetlen veszélye áll fenn és az általános adatvédelmi rendelet rendelkezései alapján bírság kiszabásának van helye.

88. Az Ákr. 103. § (1) bekezdése alapján az Ákr.-nek a kérelemre indult eljárásokra vonatkozó rendelkezéseit az Ákr. 103. és 104. §-ában foglalt eltérésekkel kell alkalmazni.

89. Az Infotv. 60/A. § (1) bekezdése alapján az adatvédelmi hatósági eljárásban az ügyintézési határidő százötven nap, amely határidőbe nem számít bele a tényállás tisztázásához szükséges adatok közlésére irányuló felhívástól az annak teljesítéséig terjedő idő.

90. Jelen eljárásban a Hatóság és az Ügyfél között a következő időpontok között zajlott a tényállás tisztázása: 2022. november 14. és 2022. november 30. napja, 2022. december 19. és 2023. január 16. napja, 2023. február 16. és 2023. március 8. napja, 2023. június 12. és 2023. június 23. napja, 2023. október 13. és 2023. október 30. napja, 2023. október 26. és 2023. november 7. napja, valamint 2023. november 23. és 2023. december 8. napja. A Hatóság és NISZ Zrt. között pedig az alábbi időpontok között zajlott a tényállás tisztázása: 2022. december 19. és 2023. január

16. napja, 2023. február 16. és 2023. március 3. napja, valamint 2023. március 17. és 2023. május 16. napja.

91. Az Ákr. 103. § (4) bekezdése szerint, ha a hatóság a hivatalbóli eljárásban az ügyintézési határidő kétszeresét túllépi, a jogsértés tényének megállapításán és a jogellenes magatartás megszüntetésére vagy a jogszerű állapot helyreállítására kötelezésen túl egyéb jogkövetkezményt nem alkalmazhat. Ez esetben ugyanazon ügyféllel szemben, ugyanazon ténybeli és jogi alapon nem indítható új eljárás.

92. Az Infotv. 61. § (1) bekezdés a) pontja alapján a Hatóság a 2. § (2) és (4) bekezdésében meghatározott adatkezelési műveletekkel összefüggésben az általános adatvédelmi rendeletben meghatározott jogkövetkezményeket alkalmazhatja.

93. Az általános adatvédelmi rendelet 58. cikk (2) bekezdés b) és i) pontja alapján, a felügyeleti hatóság korrekciós hatáskörében eljárva elmarasztalja az adatkezelőt vagy adatfeldolgozót, ha adatkezelési tevékenysége megsértette a rendelet rendelkezéseit, illetve a 83. cikknek megfelelően közigazgatási bírságot szab ki, az adott eset körülményeitől függően az e bekezdésben említett intézkedéseken túlmenően vagy azok helyett. Ugyanezen cikk (2) bekezdés d) pontja alapján, a felügyeleti hatóság korrekciós hatáskörében eljárva utasítja az adatkezelőt vagy az adatfeldolgozót, hogy adatkezelési műveleteit – adott esetben meghatározott módon és meghatározott időn belül – hozza összhangba a rendelet rendelkezéseivel.

94. A közigazgatási bírság kiszabására vonatkozó feltételeket az általános adatvédelmi rendelet 83. cikke tartalmazza. Az általános adatvédelmi rendelet 32-33. cikkének megsértése esetén a kiszabható bírság felső határa az általános adatvédelmi rendelet 83. cikk (4) bekezdés a) pontja alapján a 10 000 000 eurónak (EUR), illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 %-át kitevő összeg.

95. A határozatra egyebekben az Ákr. 80. és 81. §-át kell alkalmazni.

III. Döntés

Adatbiztonsággal kapcsolatos megállapítások

96. A Hatóság az eljárás során kiemelten vizsgálta, hogy a Kötelezett mennyiben tett eleget az incidens bekövetkezésével közvetlenül összefüggő adatbiztonsági követelményeknek **a saját fejlesztői környezete, rendszere, és a KRÉTA rendszer éles és teszt adatbázisainak onnan való elérése tekintetében.** Az nem képezte az eljárás tárgyát, hogy az éles, **publikus KRÉTA rendszerhez a diákok, szülők, tanárok által történő hozzáférés során milyen adatbiztonsági beállítások kerülnek alkalmazásra.**

97. Az általános adatvédelmi rendelet 32. cikk (1) bekezdésében foglaltak alapján az adatkezelőnek a kockázat mértékének megfelelő szintű adatbiztonság garantálása érdekében a tudomány és technológia állásának megfelelő technikai és szervezési intézkedéseket kell végrehajtania, ide értve a rendelet a 32. cikk (1) bekezdés b) pontja alapján a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét.

98. Az általános adatvédelmi rendelet 32. cikk (2) bekezdése értelmében a biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok

véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

99. Az általános adatvédelmi rendelet 28. cikk (1) és (3) bekezdése értelmében, ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés e rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. Az adatfeldolgozó által végzett adatkezelést az uniós jog vagy tagállami jog alapján létrejött olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó –szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben. A szerződés vagy más jogi aktus különösen előírja, hogy az adatfeldolgozó: […] c) meghozza a 32. cikkben előírt intézkedéseket; […].

100. Mint a fenti bekezdésben látható, az általános adatvédelmi rendelet az adatbiztonsági követelményeknek való megfelelés vonatkozásában nem tesz különbséget adatkezelő és adatfeldolgozó között, a hivatkozott rendelkezések ugyanúgy vonatkoznak az adatfeldolgozókra is, mint az adatkezelőkre.

101. Kulcsfontosságú a Kötelezett által alkalmazott adatbiztonsági beállítások, és a Kötelezett incidenskezelési intézkedéseinek a Hatóság általi értékelése során, hogy a KRÉTA rendszer éles és teszt adatbázisai, melyekhez az érintett felhasználónak is volt hozzáférése, az összes tanuló, pedagógus, gondviselő személyes adatait tartalmazzák (ld. 59-60. bekezdésekben szereplő táblázatok), ezek között ráadásul van számos olyan, melyek nyilvánosságra kerülése az érintettet különösen hátrányosan érintheti, pl. küzd-e a tanuló beilleszkedési, tanulási, magatartási, nevelési nehézséggel; sajátos nevelési igényű-e; államilag gondozott-e; részesül-e szociális támogatásban vagy rendszeres gyermekvédelmi kedvezményben. Bár nem kötelező elem, de akár a tanuló vallása is megjelenhet a KRÉTA rendszerben. A KRÉTA rendszerben ráadásul a személyes adatok nagyszámú érintettre kiterjedően és nagy mennyiségben kerülnek tárolásra: kb. 225 ezer alkalmazott, másfélmillió diák és 1.87 millió gondviselő személyes adata található meg a rendszerben. Ez a személyes adatok mennyiségét illetően összesen az alkalmazottak esetében ~6.5 millió, diákok esetében ~47 millió, gondviselők esetében pedig ~7.5 millió személyes adatot jelent. Éppen ezért hatalmas jelentőséggel bír, hogy a Kötelezett munkatársai, mint fejlesztők, hogyan férnek hozzá a fejlesztői környezethez és az éles- és tesztrendszer adatbázisaihoz, hiszen ők szolgáltatás szinten is elérik azokat.

102. Az érintett felhasználó a feltárt tényállás alapján support tevékenységet is ellátott, ebből következően minden olyan jogosultsággal rendelkezett, amely szükséges ahhoz, hogy az éles és teszt KRÉTA rendszerekhez, ill. azok adatbázisaihoz hozzáférjen. A Kötelezett úgy tájékoztatta a Hatóságot, hogy az érintett felhasználó a levelezéshez, belső kommunikációt támogató chatrendszerhez, a rendszer forráskódjait tároló külön rendszerhez, support rendszerhez fért hozzá állandó jelleggel, illetve a support feladatai ellátása kapcsán időlegesen hozzáfért az éles KRÉTA rendszerben személyes adatokhoz.

103. A Kötelezett az eljárás során szintén nyilatkozta, miszerint sokszor előfordul, hogy éles adatokkal dolgozik, az érintett felhasználó gépén is számos éles rekord volt megtalálható, amit support tevékenysége során az éles rendszerből töltött le. A KRÉTA rendszerből korábban tesztelés céljából lementett, az érintett felhasználó gépén a támadás időpontjában éppen elérhető személyes adatok számáról és mennyiségéről a Kötelezett azt nyilatkozta, hogy 12 darab szakképzési centrumhoz kapcsolódóan szerepelnek személyes adatok, összesen – a Kötelezett

által a Hatóság részére megküldött excel táblázatban szereplő adatok szerint – 8574 tanuló ~290.000 adata, 11.082 gondviselő ~44.000 adata, valamint 1205 alkalmazott ~35.000 adata.

104. Mivel a Kötelezett a helyszíni szemle alkalmával az érintett felhasználó felhasználói azonosítójával, az érintett időszakból (2022. szeptember 14. - 2022. november 8.) történt hozzáférések naplófájljait átadta a Hatóság részére, és ezekben az éles KRÉTA rendszer cél IP címei megtalálhatóak voltak, **egyértelműen megállapítható, hogy az érintett felhasználó hozzáfér*het*ett, és hozzá is fért az éles KRÉTA szerverekhez**. Ehhez egyébként jogosultsága is volt, mivel – mint azt válaszában szintén kifejtette a Kötelezett - felhasználói szintű hozzáféréssel ugyan nem rendelkezik a Kötelezett a KRÉTA rendszerhez, de a KRÉTA rendszer mögött futó adatbázisokhoz, logolási rendszerekhez, alkalmazás szerverekhez VPN kapcsolaton keresztül az együttműködési megállapodásban részletezett feladatok ellátása érdekében - kizárólag nevesített felhasználókkal, szükséges és elégséges jogosultságokkal - *hozzáfér.* A Kötelezett által megküldött, az érintett felhasználó jogosultságait tartalmazó excel táblázatok megerősítik, hogy a KRÉTA szerverekhez szerkesztési joggal hozzáfért az érintett felhasználó, ill. eKRÉTA – Database csoporttag volt, valamint […] szerver hozzáféréssel is rendelkezett, a Database Team tagjaként.

105. Ahogy a Kötelezett megbizonyosodott a támadásról 2022 szeptemberében, azonnal lecserélte az érintett felhasználó gépét, és inaktiválta mind az eredeti felhasználói fiókját, mind pedig a különféle jogosultságait, majd részére új felhasználói fiókot hozott létre. Ugyanakkor az érintett felhasználó mind a régi, mind az új felhasználójához tartozó belépési adatokat (felhasználói neveket és jelszavakat) a Google Ireland Ltd. (továbbiakban: Google) egyik szolgáltatásaként nyújtott jelszókezelőbe szinkronizálta, kivéve - nyilatkozata szerint – a NISZ-es hozzáféréshez szükséges belépési adatait. A Google jelszókezelő szolgáltatása úgy működik, hogy a használója a saját Google fiókjába mentheti a más weboldalakon elérhető alkalmazások, rendszerek eléréséhez szükséges felhasználói neveket és jelszavakat. Ha a jelszavait ilyen módon tároló felhasználó Google fiókjához illetéktelenek férnek hozzá, akkor az ott tárolt valamennyi felhasználói nevet és jelszót képesek megismerni. A jelszókezelő által biztosított szinkronizálás révén, ha valamely más weboldalhoz, rendszerhez a felhasználó a már mentetthez képest eltérő, új jelszót ad meg, akkor a Google jelszókezelője ezt képes eltárolni, vagyis a régi jelszót felülírni az újjal. A támadók az érintett felhasználó Google fiókját érhették el továbbra is, egy nyitva maradt munkamenet[3] (ún. *session*) révén, és így szerezték meg a Kötelezett valamennyi olyan rendszeréhez tartozó jelszavakat, amelyeket ugyancsak a jelszókezelőben tárolt. A Google jelszókezelőjének alkalmazása ilyenformán a KRÉTA rendszerben tárolt adatok biztonságára nézve egy kezeletlen kockázatot jelentett. A támadók az érintett felhasználó Google fiókjába már azt megelőzően beléphettek, hogy a KRÉTA rendszerhez új felhasználói fiókot és jelszót kapott, és ott ezután is bent maradhattak, köszönhetően annak, hogy a Google szervere és a támadók számítógépe között folyamatosan nyitott volt a kapcsolat (munkamenet). Ebből következően önmagában a KRÉTA rendszerhez új felhasználói fiók létrehozása ez esetben nem lehetett elégséges lépés, mivel annak jelszavát az érintett felhasználó általi első sikeres belépést követően a Google jelszókezelője szinkronizálta. A Hatóság álláspontja szerint egy ilyen jellegű tevékenységet ellátó munkatárs esetén mind a jelszavak Google szinkronizációja, mind az a tény, hogy a session nem kerül automatikusan kiléptetésre, súlyos adatbiztonsági hibának minősül, ezek elfogadhatatlan mértékben növelték a rendszer kitettségét, hiszen léteznek olyan, csak az adott számítógépre telepített jelszókezelő szoftverek, amelyekben – mint egy széfben – biztonságosan tárolhatóak a felhasználók jelszavai. Az ezekben a szoftverekben tárolt jelszavak általában csak a felhasználó kétfaktoros azonosítása, vagy rendkívül erős (azaz kellően hosszú,

[3] A munkamenet (angolul session) a számítógép-hálózatoknál két számítógép közötti kommunikáció olyan formája, mely során az egyik (vagy mindkét) gép átmenetileg adatokat tárol a másikról.

számok, kis- és nagy betűk, illetve különleges karakterek belefoglalását kikényszerítő) jelszó megadása mellett érhetőek el.

106. A támadó tehát - a Kötelezett által is elismert módon - hozzáfért az érintett felhasználó jogosultságaihoz, ebből következően megállapítható, hogy a támadó hozzáférhetett az éles KRÉTA rendszerben tárolt adatokhoz is. Az a körülmény, hogy a támadó konkrétan meg is ismerte-e az éles KRÉTA rendszerben tárolt személyes adatokat, nem volt az eljárás során bizonyítható, tekintettel arra, hogy a támadó, amennyiben belépett az éles KRÉTA rendszerbe, azt érvényes jogosultságokkal, az érintett felhasználó jogosultságaival tette, így pusztán a naplófájlok böngészése alapján nem választhatóak el a támadó lépései az érintett felhasználó lépéseitől. Az mindenesetre tényként kezelhető, hogy a támadónak megvolt a lehetősége az éles KRÉTA rendszerben tárolt adatokhoz való hozzáférésre. Ezen hozzáférés lehetőségét a Kötelezett sem zárta ki válaszaiban. Itt érdemel említést az a Kötelezett által említett információ (ld. 46. bekezdés), miszerint egy külső állami tulajdonú vállalkozó 2023 december végéig vizsgálatot folytat a Kötelezett részére, melynek keretében a KRÉTA rendszer felhasználóira vonatkozó adatok felderítését célzó keresést folytat az ún. dark weben. A Hatóság ezzel kapcsolatban hangsúlyozza, hogy amennyiben ezen keresés azon eredményre jutna is, hogy a dark weben nem találhatóak meg a KRÉTA rendszer felhasználóinak személyes adatai, az sem lenne bizonyító erejű arra nézve, hogy a támadók nem mentettek ki személyes adatokat a KRÉTA rendszerből, hiszen nem törvényszerű, hogy a támadók a támadás során esetlegesen megszerzett információkat közzé is teszik később.

107. A tényállás meghatározó eleme, hogy az éles KRÉTA rendszer eléréséhez a kétfaktoros autentikáció beállítására a jelen határozat 32. bekezdésében említettek szerint a Kötelezett csak 2022. november 10. napján kerített sor.

A kétfaktoros hitelesítés (2FA) egy identitás- és hozzáférés-kezelési biztonsági módszer, amely kétféle azonosítást igényel az erőforrások és az adatok eléréséhez. A kétfaktoros hitelesítés lehetővé teszi a vállalkozások számára a legsérülékenyebb információk és hálózatok figyelését és védelmének biztosítását. A kétfaktoros autentikálás hiánya miatt a felhasználói név és jelszó párosának jogosulatlan személy általi megismerése esetén az ilyen jogosulatlan személyek is sikeresen beléphetnek az egyes rendszerekbe. Épp ezért számít általánosan elterjedt jó gyakorlatnak a jelszón, mint „faktoron” kívül egy második faktor – például egyszer használatos kódszó SMS-ben történő kiküldése, vagy hardveres azonosító (ún. token) – alkalmazása is. Míg egy jelszó kellő számú próbálkozással „kitalálható”, azaz visszafejthető, addig egy rövid lejárati idővel használható kódszó, illetve csakis a jogosult személy által birtokolt hardveres token nem.

108. A kockázat mértékének megfelelő szintű adatbiztonság garantálására vonatkozó kötelezettség miatt **az adatbiztonság követelményének fokozottan érvényesülnie kell egy olyan rendszer esetén, amilyen a Kötelezett fejlesztői környezete**, hiszen – bár abban is tárolásra kerülnek az éles KRÉTA rendszerből származó személyes adatok a support tevékenység ellátása kapcsán, nem is kis számban – onnan a feladatellátás miatt könnyedén elérhető az éles KRÉTA rendszer adatbázisa, amelyben a fentebb részletezettek szerint nagyszámú érintettre kiterjedően és nagy mennyiségben kerülnek tárolásra személyes adatok.

109. A tény, hogy az ügy tárgyát képező incidens bekövetkezett, és annak súlyosságáról a Kötelezett nem is maga szerzett tudomást, hanem csak a támadó üzenete által, több, mint másfél hónappal a biztonság sérülését követően, lényeges bizonyítéka annak, hogy a Kötelezettnél az általános adatvédelmi rendelet adatbiztonsági előírásai nem teljesültek megfelelően.

110. A 2022 szeptemberben közepén észlelt adathalász támadás kivizsgálása során a Hatóság álláspontja szerint a Kötelezett - közvetlenül a támadás 2022 szeptemberi észlelését követően -

nem folytatott az érintett munkavállalóhoz kapcsolódó információbiztonsági kockázatok teljeskörű felmérése érdekében kellő mélységű vizsgálatot, válaszintézkedései szinte kimerültek abban, hogy az adott felhasználói fiókot törölte, és az érintett felhasználó jogosultságait felfüggesztette. Amennyiben erre a vizsgálatra – különösen az éles KRÉTA rendszerben tárolt személyes adatok mennyiségét és érzékenységét is figyelembe véve – a kellő gondosság mellett sor került volna, úgy a Kötelezettnek az információbiztonsági jó gyakorlatokat követve legalább az érintett felhasználóhoz kapcsolódó hálózati forgalmat figyelnie kellett volna *huzamosabb ideig*, és az adott felhasználó bevonásával kellett volna vizsgálnia azt is, hogy mely forgalom köthető az ő tevékenységéhez és melyik ismeretlen – így vélelmezhetően illetéktelen – felhasználókhoz. Erre már csak azért is szükség lett volna, mivel a Kötelezettnek nem volt kellő információja arról, hogy sor került-e jogosulatlan hozzáférésre, így az esemény okainak és potenciális következményeinek a teljes körű kivizsgálása elvárható lett volna a részéről. Ha erre sor került volna, akkor a Kötelezett vélhetően időben észlelte volna, hogy illetéktelenek tartózkodnak a rendszereiben, úgyszintén azt is, hogy pontosan mihez fértek hozzá, és így jó eséllyel elkerülhették volna a helyzet további súlyosbodását.

111. A fentiek pontosan megvilágítják a tényállás egyik meghatározó elemét, mégpedig azt, hogy miért lett volna kiemelt jelentőségű, és akadályozhatta volna meg az incidenst, ha a Kötelezett informatikai fejlesztői környezetében használt rendszerekhez – legalább amelyekben személyes adatok szerepelnek – már a támadás időpontjában is csak kétfaktoros hitelesítést követően lehetett volna hozzáférni, és az éles KRÉTA rendszer eléréséhez a kétfaktoros autentikáció beállítására a Kötelezett nem csak 2022 novemberében kerített volna sort.

112. Megállapítható az is, hogy az a naplózás, amelyet a Kötelezett a munkatársainak tevékenysége kapcsán végzett, az incidens kivizsgálása szempontjából elégtelennek bizonyult, hiszen – mint ahogyan az jelen esetben is történt – ha egy támadó hozzáférést szerzett valamely munkatárs profiljához, onnantól kezdve a támadó bármit csinálhatott, akár minden adatot (beleértve ez esetben az éles KRÉTA rendszerben szereplő adatokat is) kimenthetett, a támadó tevékenységét onnantól kezdve nem lehetett elválasztani a feltört profil tulajdonosának tevékenységétől. Ez súlyos adatbiztonsági hiányosság, hiszen ilyen naplózással lehetetlen eleget tenni az általános adatvédelmi rendelet 32. cikk (1) bekezdés b) pontjában és 32. cikk (2) bekezdésében megfogalmazott követelményeknek. A Hatóság ismét hangsúlyozza, hogy a Kötelezett az eljárás során semmi olyan információt nem prezentált, amely bizonyító erővel rendelkezett volna azzal kapcsolatban, hogy a támadás során az éles KRÉTA rendszerből nem mentettek le adatokat.

113. A fentiekből következően egyértelműen megállapítható tehát, hogy egy KRÉTA szintű rendszer fejlesztése során minimum elvárás a kétfaktoros hitelesítés, valamint egy esetleges biztonsági incidens kivizsgálása esetén a történtek felderítéséhez elegendő tartalmú naplózás megléte. A Hatóságot számára nem az bír jelentőséggel, hogy a Kötelezett által végzett naplófájlok pontosan milyen rekordokat tartalmaznak, hanem az, hogy ezen rekordok alapján lehetséges-e a biztonsági esemény kellő mélységű feltárása. Ez utóbbi kérdésre nemleges válasz adandó jelen ügyben, és a kétfaktoros autentikáció is csak a támadást követően került bevezetésre, mely körülmények jelentős mértékben hozzájárultak a támadás sikerességéhez, valamint ahhoz, hogy a Kötelezett nem volt képes időben felismerni a jogosulatlan hozzáférés tényét, illetve annak mértékét, és így nem tudta időben elkezdeni a kockázatcsökkentő intézkedések implementálását sem.

114. A Hatóság határozottan nem osztja a Kötelezettnek azt az álláspontját, miszerint az incidens csupán egy munkatársának gondatlanságából fakadt, az incidens ezért nem vezethető vissza komoly adatbiztonsági problémára. Bár az incidens közvetlen kiváltó oka valóban munkavállalói hiba volt, megfelelő adatbiztonsági intézkedések mellett ez semmiképpen nem járt volna az ügyben ismertetett következményekkel. A Kötelezett saját álláspontjának is ellentmond azzal,

hogy az **incidensről való 2022 novemberi tudomásszerzést követően jelentős számú (közel húsz!), rendszerszintű változásokat is tartalmazó, alapvető fontosságú és a technológia állása szerint is elvárható intézkedést vezetett be (ld. 76. bekezdés), holott amennyiben valóban úgy gondolná, hogy egy munkavállói figyelmetlenség volt pusztán az incidens kiváltója, erre nem lett volna oka**. Bár a felhasználói tudatosságnövelés valóban elvárható egy olyan szintű cégtől, mint amilyen a Kötelezett, hiszen egy vállalkozás sem építhet arra, hogy a munkavállalója 'úgysem fog hibázni', ez csak a potenciális adatbiztonsági intézkedéseknek egy kicsi, bár fontos szeletét képezi, szükségesek emellett az egyéb adatbiztonsági intézkedések is, mint ahogyan ezt a Kötelezett által utólag megtett, és a 76. bekezdésben részletesen ismertetett intézkedések is demonstrálják.

115. A fentiekre tekintettel a Hatóság megállapítja, hogy a Kötelezett nem tett eleget az általános adatvédelmi rendelet 32. cikk (1) bekezdés b) pontjában, valamint a 32. cikk (2) bekezdésében foglalt kötelezettségének azáltal, hogy az informatikai fejlesztői környezetének adatbiztonsági beállításai során nem vette kellőképpen figyelembe az adatkezelésből eredő olyan kockázatokat, amelyek a személyes adatok jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek, és emiatt a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét nem garantálta.

Az adatvédelmi incidens kezelése, kockázati besorolása és bejelentése

116. Az általános adatvédelmi rendelet 4. cikk 12. pontja értelmében „adatvédelmi incidens": a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

117. Adatvédelmi incidens vizsgálata esetén az incidens kezelése során tett lépések értékelése elválaszthatatlan az adatkezelő / adatfeldolgozó rendszereinek adatbiztonsági beállításaitól, az adatbiztonsági környezet sajátosságaitól. Mivel az ügy tárgyát képező incidens be sem következett volna megfelelő adatbiztonsági háttér mellett, az alábbi megállapítások a fentebb a Hatóság által az adatbiztonsággal kapcsolatban kifejtettekkel összefüggésben, azok fényében értelmezendők.

118. A Hatóság az adatvédelmi incidensek súlyosságát elsősorban a biztonsági sérülésnek az érintett természetes személyek jogaira és szabadságaira jelentett kockázat szintje alapján értékeli. Összességében a korábban kifejtettekkel összhangban megállapítható, hogy egy vállalkozásnak, amely olyan jellegű rendszert fejleszt, mint a KRÉTA rendszer (mely több millió természetes személy több tízmillió személyes adatát tartalmazza, ld. 61. bekezdés), és bír az abban tárolt, az 59-60. bekezdésben ismertetett adatokhoz hozzáféréssel, már csak erre tekintettel is, a legkisebb biztonsági sérülésre utaló jelet is a lehető legkomolyabban kell vennie és kivizsgálnia. Különösen igaz ez akkor, amikor *ténylegesen* egy olyan profillal kapcsolatban merül fel a támadás lehetősége/esélye, amelyről az éles KRÉTA rendszerhez is hozzáférhetnek.

119. Az általános adatvédelmi rendelet 32. cikk (1) bekezdésének értelmében az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

120. A kétfaktoros autentikáció hiánya és a Kötelezett által végzett naplózás fentebb részletezett hiányosságai a fejlesztői környezetben semmiképpen nincsenek összhangban a tudomány és a technológia állásával. A Kötelezett által fejlesztett rendszerben tárolt, illetve adott esetben a support tevékenység körében lementett személyes adatok mennyisége jól meghatározza az adatkezelés jellegét és hatókörét, ilyen rendszer fejlesztése esetén minimum elvárás, hogy a tudomány és technológia legújabb állásának megfelelő, minden észszerűen elérhető adatbiztonsági intézkedésnek érvényt kell szerezni. A Kötelezett által *az incidens bekövetkezését* ***követően*** megtett, a 76. bekezdésben részletesen ismertetett adatbiztonsági jellegű intézkedéseket a Hatóság megfelelőnek ítélte, ez is csak azt támasztja alá azonban, hogy a Kötelezett tisztában van azzal, hogy milyen szintű és jellegű adatbiztonsági intézkedések lennének elvárhatóak egy olyan rendszer esetében, mint amelyet fejleszt, mégis jelen incidensnek kellett bekövetkeznie ahhoz, hogy ezek meg is valósuljanak.

121. Az alapján, hogy milyen személyes adatokhoz történt / történhetett hozzáférés a támadó részéről, a Kötelezettnél bekövetkezett adatvédelmi incidens a Hatóság álláspontja szerint két szinten értelmezhető:

122. *Az incidens első szintje:* A támadás bizonyítottan érintette azokat a személyes adatokat, amelyeket az érintett felhasználó a support tevékenységével kapcsolatban mentett le a gépére, illetve a Kötelezett munkavállalóinak adatait (ld. 45-46. bekezdés). **Ez esetben** – az érintettek magas száma és az érintett személyes adatok nagy mennyisége miatt - **bizonyíthatóan megvalósult egy magas kockázatú adatvédelmi incidens**.

123. *Az incidens második szintje:* az éles KRÉTA rendszerben szereplő személyes adatokhoz való potenciális hozzáférés a támadó részéről. Ezzel kapcsolatban a határozat fenti, a Kötelezett adatbiztonsági beállításait elemző része tartalmazott megállapításokat, de a Hatóság itt ismételten ki kívánja emelni, hogy a Kötelezett az eljárás során nem mutatott be semmiféle olyan információt, amely minden kétséget kizáróan bizonyítaná, hogy a támadó az éles KRÉTA rendszerből nem mentett ki személyes adatokat. A Hatóság álláspontja szerint az eljárás során feltárt információk alapján összességében megalapozottan lehet arra következtetni, hogy a támadás során hozzáfértek az éles KRÉTA rendszerben tárolt személyes adatokhoz is. **A magas kockázatú adatvédelmi incidens bekövetkezése ebben az esetben tehát valószínűsíthető.**

124. Válaszában a Kötelezett úgy fogalmazott, hogy az őt ért támadás feltehetően 2022. szeptember 15. napján valósult meg, ekkor nyitotta meg az érintett munkavállaló a fertőzött elemet, egy adathalász üzenetet. A 40. bekezdésben részletezettek alapján 2022. szeptember 19. napján jelezte az érintett felhasználó a problémát a felettesének és az üzemeltetési csoportvezetőnek, a Hatóság ezért az adatvédelmi incidensről való tudomásszerzés időpontjának ezt a napot tekinti. Bár a Kötelezett ekkor képtelen volt a támadás valós kiterjedését és következményeit felmérni, már ekkor tudomása volt róla, hogy adathalász támadás áldozatául esett, tehát kellő gondosság mellett legalább feltételeznie kellett volna az előző két bekezdésben említett következmények bekövetkezésének lehetőségét. A Hatóság nem értékelheti a Kötelezett javára, hogy saját hanyagsága miatt ezen feltételezéssel nem élt, és képtelen volt olyan belső vizsgálatot lefolytatni, amellyel már 2022 szeptemberében megbizonyosodhatott volna arról, hogy milyen kiterjedésű volt a támadás, mely egyébként adathalász támadás révén nem volt egy nehezen detektálható, szofisztikált támadás.

125. Mivel a Hatóság értékelése szerint a Kötelezett már 2022 szeptember 19. napján tudomást szerzett minimum a 122. bekezdésben említett adatvédelmi incidensről, az általános adatvédelmi rendelet 33. cikk (2) bekezdése értelmében kötelessége lett volna a tudomásszerzését követően indokolatlan késedelem nélkül bejelenti azt az adatkezelőknek, vagyis jelen esetben annak a 12

intézménynek (ld. 45. bekezdés), amelyekhez tartozó személyes adatok le voltak mentve support tevékenység körében az érintett felhasználó gépére.

126. Az incidens fenti körülményeit összesítve, a Kötelezettnél egymással összefüggő okokból bizonyíthatóan bekövetkezett egyrészről egy magas kockázatú incidens, másrészről valószínűsíthetően bekövetkezett egy kiemelkedően magas kockázatú incidens. Bár az adatvédelmi incidensek kockázatainak felmérése tipikusan az adatkezelő feladata, ez esetben a KRÉTA rendszer, és a fejlesztői környezet jellegéből kifolyóan a Kötelezett, mint adatfeldolgozó volt csak abban a helyzetben, hogy az eset összes körülményének ismeretében az incidens kockázatait fel tudja mérni.

127. A fentiekre tekintettel a Hatóság megállapítja, hogy a Kötelezett megsértette az általános adatvédelmi rendelet 33. cikk (2) bekezdését, mert egy olyan adatvédelmi incidenst, amellyel kapcsolatban
   a) a támadás ténye (az érintett felhasználó rákattintott az adathalász üzenetben levő linkre) 2022 szeptember 19. napján már ismert volt a Kötelezett előtt,
   b) a támadás sikerességéről, következményeiről pedig - a rendszer jellege és hatóköre alapján - jogosan elvárható vizsgálati intézkedések megtétele esetén rövid úton megbizonyosodhatott volna,

   nem jelentett be indokolatlan késedelem nélkül az adatkezelőknek.

Az alkalmazott szankció és indoklása

128. A Hatóság a tényállás tisztázása során megállapította a Kötelezett vonatkozásában, hogy az adatkezelése során
   - megsértette az általános adatvédelmi rendelet 32. cikk (1) bekezdésének b) pontját, valamint a 32. cikk (2) bekezdését,
   - megsértette az általános adatvédelmi rendelet 33. cikk (2) bekezdését.

129. A Hatóság megvizsgálta, hogy indokolt-e a Kötelezettel szemben adatvédelmi bírság kiszabása. E körben a Hatóság a GDPR 83. cikk (2) bekezdése és az Infotv. 75/A. §-a alapján mérlegelte az ügy összes körülményét.

130. Erre tekintettel a Hatóság az Infotv. 61. § (1) bekezdés a) pontja alapján a rendelkező részben foglaltak szerint döntött, és jelen határozatban a Kötelezettet adatvédelmi bírság megfizetésére is kötelezte.

131. A Hatóság a bírság kiszabása során az alábbi tényezőket vette figyelembe:

132. A Hatóság súlyosító körülményként vette figyelembe a következőket:

133. Az incidenssel érintett adatok kezelése az adatok mennyiségéből és jellegéből (ld. 59-61. bekezdések) fakadóan kiemelkedően magas kockázattal jár, ezért a Kötelezettnek fokozott elővigyázatossággal kellett volna eljárnia a kockázat mértékének megfelelő szintű adatbiztonság garantálása érdekében. A Kötelezett ennek ellenére a nagyszámú érintettre kiterjedő, nagy mennyiségű személyes adat kezelésére használt rendszere folyamatos bizalmas jellegének biztosítása érdekében nem hozott az incidenst megelőzően megfelelő intézkedéseket. A jogsértés az elvárható adatbiztonsági intézkedések megléte esetén vagy be sem következett volna, vagy már 2022 szeptemberében megszüntetésre kerülhetett volna. A feltárt tényállás alapján ugyanakkor az incidens súlyának és az adatbiztonsági hiányosságok tényleges mértékének felismerésére csak 2022 novemberében került sor (általános adatvédelmi rendelet 83. cikk (2) bekezdés a) és g) pont).

134. A Hatóság a feltárt tényállás alapján megállapította, hogy a Kötelezett felróható, gondatlan magatartása vezetett a fenti jogsértésekhez, a Kötelezettnek az általa fejlesztett rendszer ismertsége és a benne tárolt személyes adatok mennyisége miatt is számítania kellett külső támadásokra, az általános adatvédelmi rendelet 32. cikkében említett technikai és szervezési intézkedések kötelezettsége pedig az informatikai támadások sikerességének elkerülés érdekében is került meghatározásra. Az a tény azonban, hogy a 76. bekezdésben ismertetett intézkedéseket csak az incidens bekövetkezése után vezette be a Kötelezett, arra utal, hogy a Kötelezett könnyelműen bízott a támadások elmaradásában, és egy alapvetően magas kockázatú adatkezelés tekintetében a jogosulatlan hozzáférések kiküszöbölésére és kimutatására alkalmatlan, a kockázatokkal aránytalan adatbiztonsági intézkedéseket alkalmazott. Az 59-61. bekezdésekben említett kategóriájú és mennyiségű személyes adatok kezelésére való biztonsági felkészültség a Kötelezettől, mint profit alapú vállalkozástól fokozottan elvárható (általános adatvédelmi rendelet 83. cikk (2) bekezdés b), c) és d) pont).

135. Arra, hogy a támadó mit kezd a támadás során megszerzett személyes adatokkal, nincs további ráhatása a Kötelezettnek, ez a körülmény pedig a személyes adatok további sorsával kapcsolatban nagy mértékű bizonytalanságra ad okot (általános adatvédelmi rendelet 83. cikk (2) bekezdés a) pont).

136. A Hatóság az adatvédelmi incidensről nem a Kötelezett által, hanem a médiában megjelent hírek alapján szerzett tudomást (általános adatvédelmi rendelet 83. cikk (2) bekezdés h) pont).

137. A Hatóság enyhítő körülményként vette figyelembe a következőt:

138. A Hatóság figyelembe vette, hogy a Kötelezettel szemben korábban nem állapított meg hasonló jogsértést a személyes adatok kezelésével kapcsolatban, illetve vele szemben korábban – ugyanebben a tárgyban – nem rendelte el az általános adatvédelmi rendelet 58. cikk (2) bekezdésében említett intézkedések valamelyikét (általános adatvédelmi rendelet 83. cikk (2) bekezdés e) és i) pont).

139. Egyéb körülmények:

140. A Hatóság figyelemmel volt arra is, hogy a Kötelezett együttműködött a Hatósággal az ügy kivizsgálása során, noha e magatartást – mivel a jogszabályi kötelezettségek betartásán nem ment túl – nem értékelte kifejezetten enyhítő körülményként (általános adatvédelmi rendelet 83. cikk (2) bekezdés f) pont).

141. Az általános adatvédelmi rendelet 83. cikk (2) bekezdés j) pontja az ügyben nem bírt relevanciával.

142. A fentiekre tekintettel a Hatóság szükségesnek tartotta a bírság kiszabását, csupán az Infotv. 75/A. §-a szerinti figyelmeztetés alkalmazását nem tartotta megfelelőnek.

143. Az adatvédelmi bírság összegét a Hatóság jogszabályon alapuló mérlegelési jogkörében eljárva határozta meg.

144. A Kötelezett által elkövetett jogsértések az általános adatvédelmi rendelet 83. cikk (4) bekezdés a) pontja szerinti bírságkategóriába tartozó jogsértésnek minősülnek.

145. A bírság kiszabása során a Hatóság figyelembe vette a Kötelezett gazdasági súlyát is. E körben figyelembe vette, hogy a Kötelezettnek a beszámolója szerint 2022. január 1. és 2022. december

31. napja között 8.429.507.000 HUF (nyolcmilliárd-négyszázhuszonkilencmillió-ötszázhétezer forint) nettó árbevétele volt.

146. A jogsértés súlyára és a Kötelezett fenti gazdálkodási adataira tekintettel a kiszabott bírság mértéke a Hatóság megítélése szerint a jogsértés súlyával arányosnak tekinthető.

IV. Egyéb kérdések

147. A Hatóság hatáskörét az Infotv. 38. § (2) és (2a) bekezdése határozza meg, illetékessége az ország egész területére kiterjed.

148. Az Ákr. 112. §-a, és 116. § (1) bekezdése, illetve a 114. § (1) bekezdése alapján a határozattal szemben közigazgatási per útján van helye jogorvoslatnak.

149. A közigazgatási per szabályait a közigazgatási perrendtartásról szóló 2017. évi I. törvény (a továbbiakban: Kp.) határozza meg. A Kp. 12. § (1) bekezdése alapján a Hatóság döntésével szembeni közigazgatási per törvényszéki hatáskörbe tartozik, a perre a Kp. 13. § (3) bekezdés a) pont aa) alpontja alapján a Fővárosi Törvényszék kizárólagosan illetékes. A Kp. 27. § (1) bekezdés b) pontja alapján a törvényszék hatáskörébe tartozó perben a jogi képviselet kötelező. A Kp. 39. § (6) bekezdése szerint a keresetlevél benyújtásának a közigazgatási cselekmény hatályosulására halasztó hatálya nincs.

150. A Kp. 29. § (1) bekezdése és erre tekintettel a Pp. 604. § szerint alkalmazandó, az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: E-ügyintézési tv.) 9. § (1) bekezdés b) pontja szerint az ügyfél jogi képviselője elektronikus kapcsolattartásra kötelezett.

151. A keresetlevél benyújtásának idejét és helyét a Kp. 39. § (1) bekezdése határozza meg. A tárgyalás tartása iránti kérelem lehetőségéről szóló tájékoztatás a Kp. 77. § (1)-(2) bekezdésén alapul. A közigazgatási per illetékének mértékét az illetékekről szóló 1990. évi XCIII. törvény (továbbiakban: Itv.) 45/A. § (1) bekezdése határozza meg. Az illeték előzetes megfizetése alól az Itv. 59. § (1) bekezdése és 62. § (1) bekezdés h) pontja mentesíti az eljárást kezdeményező felet.

152. Az Ákr. 132. §-a szerint, ha a kötelezett a hatóság végleges döntésében foglalt kötelezésnek nem tett eleget, az végrehajtható. A Hatóság határozata az Ákr. 82. § (1) bekezdése szerint a közléssel véglegessé válik. Az Ákr. 133. §-a értelmében a végrehajtást - ha törvény vagy kormányrendelet másként nem rendelkezik - a döntést hozó hatóság rendeli el. Az Ákr. 134. §-a értelmében a végrehajtást - ha törvény, kormányrendelet vagy önkormányzati hatósági ügyben helyi önkormányzat rendelete másként nem rendelkezik - az állami adóhatóság foganatosítja. Az Infotv. 60. § (7) bekezdése alapján a Hatóság határozatában foglalt, meghatározott cselekmény elvégzésére, meghatározott magatartásra, tűrésre vagy abbahagyásra irányuló kötelezés vonatkozásában a határozat végrehajtását a Hatóság foganatosítja.

Kelt.: [elektronikus aláírás szerint]

Dr. habil. Péterfalvi Attila
elnök
c. egyetemi tanár