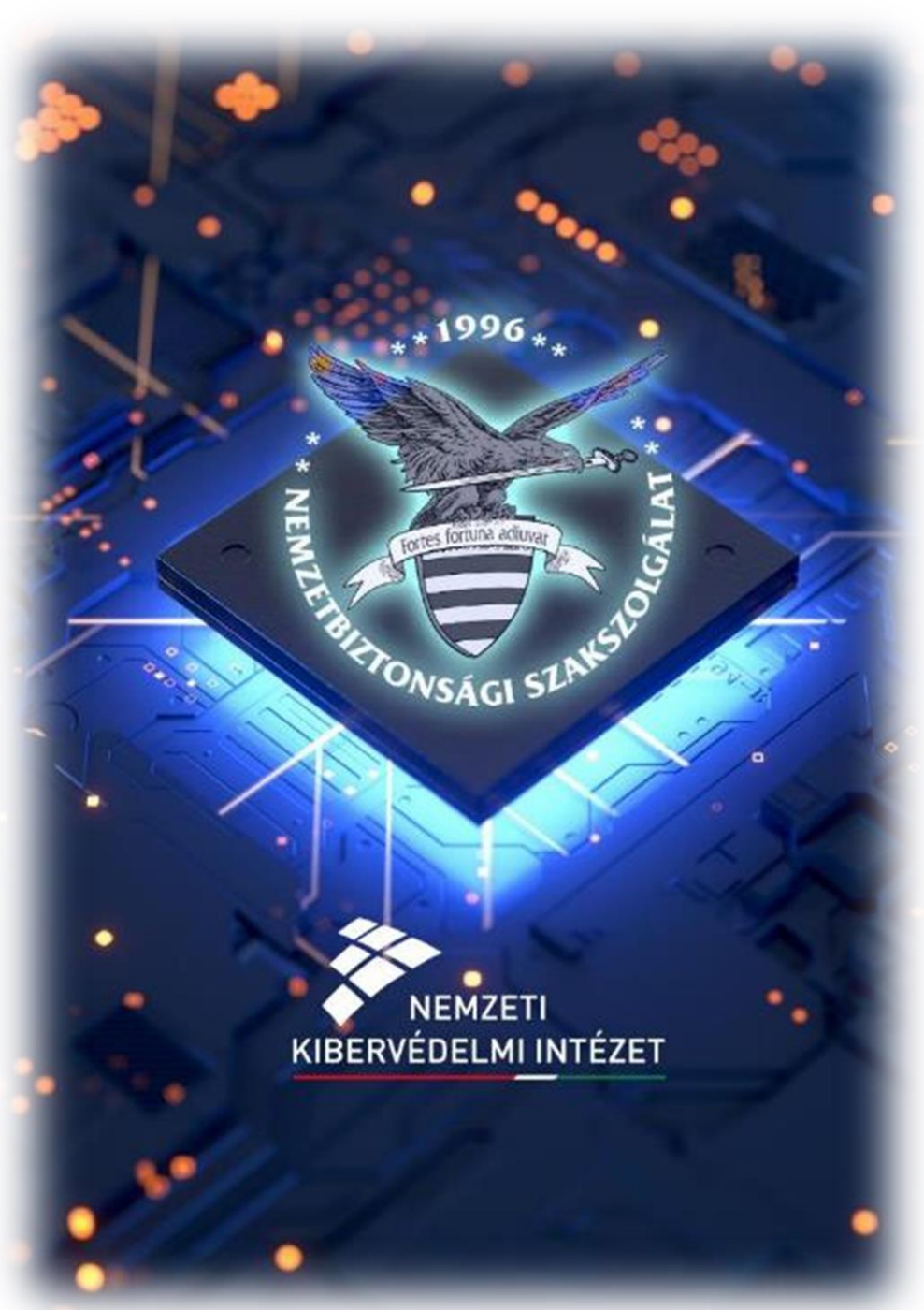

INCIDENS BEJELENTÉS

dr Munkácsi Viktor nb. alezredes
nemzetbiztonsági főtanácsos
Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet Incidenskezelési
Főosztály Vezetője E-mail:
viktor.munkacsi@nki.gov.hu
Web: nki.gov.hu

2024. november 12.

KIBERBIZTONSÁGI HATÓSÁGOK / INCIDENSBEJELENTÉS

KIBERBIZTONSÁGI HATÓSÁGOK/ESEMÉNYKEZELŐK

SZTFH

NEMZETI KIBERVÉDELMI INTÉZET

MAGYAR NEMZETI BANK

KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT – A HAZÁÉRT BECSÜLETTEL

KIBERTAN TV. ALANYOK

NIS2 ÁGAZGATOK

PÉNZÜGYI SZEREPLŐK

HONVÉDELMI ÁGAZAT

NKI KORLÁTAI

AZ NBSZ NKI-NAK NINCS NYOMOZATI JOGKÖRE

NINCS FOGYASZÓVÉDELMI HATÓSÁGI JOGKÖR

ADATVÉDELMI HATÓSÁGI JOGKÖR HIÁNYA

POLGÁRI JOGI VITÁKBAN NINCS JOGKÖRÜNK ELJÁRNI

JOGI HÁTTÉR

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE (NIS-2)
- A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

  (Jelentősnek minősülő biztonsági események)
- Magyarország kiberbiztonságáról szóló törvénytervezet
- 271/2018. (XII. 20.) Korm. rendelet

FOGALMAK

Nemzeti kiberbiztonsági incidenskezelő központ:

- Az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, kiberbiztonsági incidensekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal rendelkezik
- Európai használatban: **CSIRT** (Computer Security Incident Response Team)
- Amerikai használatban: **CERT** (Computer Emergency Response Team)];

Ágazaton belüli kiberbiztonsági incidenskezelő központ:

Az e **törvény hatálya alá tartozó** egy vagy több, **egy ágazathoz tartozó szervezetnek** az ágazaton belüli **meghatározott szakterületen előforduló kiberbiztonsági incidenseinek a központosított és egységes kezelése érdekében** üzemeltetett kiberbiztonsági incidenskezelő központja

FOGALMAK

Kiberbiztonsági incidens: Olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;

Confidentiality – Bizalmasság: A titkos információk védelme, valamint annak a biztosítása, hogy csak jogosult személyek férhessenek hozzá a fájlokhoz és a fiókokhoz.

Integrity – Integritás: A tárolt adatok valóban megfelelnek a tárolni kívánt információknak, megfelelő felhatalmazás nélkül senki ne szúrjon be, módosítson vagy töröljön semmit.

Access – Elérhetőség: Szükség szerint hozzá lehessen férni a rendszerekhez és az adatokhoz.

FOGALMAK

Üzemeltetési kiberbiztonsági incidens: Olyan kiberbiztonsági incidens, amely az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált, vagy azokon keresztül elérhető szolgáltatások **rendelkezésre állását nem szándékoltan csökkenti vagy megszünteti**

Karbantartások!

FOGALMAK

Jelentős kiberbiztonsági incidensnek: minősül az olyan kiberbiztonsági incidens, amely

a) a szolgáltatás legalább 5%-os csökkenésével vagy a szervezet éves bevételének legalább 5 %-os kiesésével jár vagy fenyeget;

b) súlyos működési zavart okoz vagy képes okozni a szolgáltatásokban, vagy pénzügyi vagy reputációs veszteséget okoz vagy képes okozni a kiberbiztonsági incidens által érintett szervezetnek vagy személynek; vagy

c) jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett, vagy képes érinteni;

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

(JELENTŐSNEK MINŐSÜLŐ INCIDENSEK)

Hatályos: 2024. november 07.

FOGALMAK

Nagyszabású kiberbiztonsági incidens: olyan kiberbiztonsági incidens, amely olyan mértékű zavart okoz, amely meghaladja Magyarországnak az arra való reagálási képességét, vagy amely Magyarországra és legalább még egy másik országra jelentős hatást gyakorol;

Kiberbiztonsági incidensközeli helyzet: olyan esemény, amely veszélyeztethette volna az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát, de amelynek bekövetkezését sikerült megakadályozni, vagy amely nem következett be;

Kiber-fizikai rendszer: olyan programozható elektronikus információs rendszerek, amelyek kölcsönhatásba lépnek a fizikai környezettel vagy kezelik a fizikai környezettel kölcsönhatásba lépő eszközöket. Ezek az elektronikus információs rendszerek közvetlenül fizikai változást érzékelnek vagy idéznek elő az eszközök, folyamatok és események megfigyelésével vagy vezérlésével;

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

3. cikk

Jelentős biztonsági események

(1) Egy biztonsági esemény az (EU) 2022/2555 irányelv 23. cikke (3) bekezdésének alkalmazásában akkor tekintendő jelentősnek az érintett szervezetek tekintetében, ha az alábbi kritériumok közül legalább egy teljesül:

a)a biztonsági esemény az érintett szervezetnek **500 000 EUR-t** vagy az előző pénzügyi évben elért teljes éves árbevételének 5 %-át (amelyik alacsonyabb) meghaladó közvetlen pénzügyi veszteséget okozott vagy okozhat;

b) a biztonsági esemény az érintett szervezet (EU) 2016/943 irányelv 2. cikkének 1. pontja szerinti üzleti titkainak kiszivárgását okozta vagy okozhatja;

c) a biztonsági esemény valamely természetes személy halálát okozta vagy okozhatja;

d) a biztonsági esemény valamely természetes személy egészségkárosodását okozta vagy okozhatja;

e) a hálózati és információs rendszerekhez olyan sikeres, gyaníthatóan rosszindulatú és jogosulatlan hozzáférés történt, amely súlyos működési zavarokat okozhat;

f) a biztonsági esemény megfelel a 4. cikkben meghatározott kritériumoknak; (ismétlődő)

g) a biztonsági esemény megfelel egy vagy több, az 5–14. cikkben meghatározott kritériumnak.

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

- Ismétlődő események
- A DNS-szolgáltatók
- A legfelső szintű doménnév-nyilvántartók
- A felhőszolgáltatók
- Az adatközpontok
- A tartalomszolgáltató hálózati szolgáltatók
- Az irányított szolgáltatók és az irányított biztonsági szolgáltatók
- Az online piacterek szolgáltatói
- Az online keresőprogramok szolgáltatói
- A közösségimédia-szolgáltatási platformok
- A bizalmi szolgáltatók

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

Ismétlődő események

- 6 hónapon belül legalább kétszer előfordultak
- ugyanahhoz a nyilvánvaló kiváltó okhoz kapcsolódnak
- együttesen 500 000 EUR-t vagy az előző pénzügyi évben elért teljes éves árbevételének 5 %-át (amelyik alacsonyabb) meghaladó közvetlen pénzügyi veszteséget okozott

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

A DNS-szolgáltatók tekintetében jelentősnek minősülő biztonsági események

- a rekurzív vagy autoritatív doménnévfeloldási szolgáltatás több mint 30 percig egyáltalán nem áll rendelkezésre

- a rekurzív vagy autoritatív doménnévfeloldási szolgáltatás DNS-kérelmekre adott válaszainak átlagos válaszideje egy óránál hosszabb ideig meghaladja a 10 másodpercet;

- az autoritatív doménnévfeloldási szolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége sérült, kivéve azokat az eseteket, amikor a DNS-szolgáltató által kezelt doménnevek legfeljebb 1 %-át képviselő, kevesebb mint 1 000 doménnév adatai pontatlanok hibás konfiguráció miatt.

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

A legfelső szintű doménnév-nyilvántartók tekintetében jelentősnek minősülő biztonsági események

- az autoritatív doménnévfeloldási szolgáltatás egyáltalán nem áll rendelkezésre
- az autoritatív doménnévfeloldási szolgáltatás DNS-kérelmekre adott válaszainak átlagos válaszideje egy óránál hosszabb ideig meghaladja a 10 másodpercet;
- a legfelső szintű doménnév-nyilvántartó technikai működésével összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége sérül.

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

A felhőszolgáltatók tekintetében jelentősnek minősülő biztonsági események

- a nyújtott felhőszolgáltatás több mint 30 percig egyáltalán nem áll rendelkezésre;

- a szolgáltató felhőszolgáltatása a felhőszolgáltatást igénybe vevő uniós felhasználók több mint 5 %-a vagy több mint 1 millió, a felhőszolgáltatást igénybe vevő uniós felhasználó számára (amelyik szám kisebb) egy óránál hosszabb ideig korlátozottan áll rendelkezésre;

- felhőszolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;

- a felhőszolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely az adott felhőszolgáltatást igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy több mint 1 millió, az adott felhőszolgáltatást igénybe vevő uniós felhasználót érint (amelyik szám kisebb).

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

Az adatközpontok tekintetében jelentősnek minősülő biztonsági események

- a szolgáltató által üzemeltetett adatközpont adatközpont-szolgáltatása egyáltalán nem áll rendelkezésre;
- a szolgáltató által üzemeltetett adatközpont adatközpont-szolgáltatása több mint egy órán át csak korlátozottan áll rendelkezésre;
- az adatközpont-szolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;
- a szolgáltató által működtetett adatközponthoz való fizikai hozzáféréssel kapcsolatban problémák merültek fel.

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

A tartalomszolgáltató hálózati szolgáltatók tekintetében jelentősnek minősülő biztonsági események

- a tartalomszolgáltató hálózat több mint 30 percig egyáltalán nem áll rendelkezésre;

- a tartalomszolgáltató hálózat a tartalomszolgáltató hálózatot igénybe vevő uniós felhasználók több mint 5 %-a vagy több mint 1 millió, a tartalomszolgáltató hálózatot igénybe vevő uniós felhasználó számára (amelyik szám kisebb) egy óránál hosszabb ideig korlátozottan áll rendelkezésre;

- a tartalomszolgáltató hálózat rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;

- a tartalomszolgáltató hálózat rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely az adott tartalomszolgáltató hálózatot igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy több mint 1 millió, az adott tartalomszolgáltató hálózatot igénybe vevő uniós felhasználót érint (amelyik szám kisebb).

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

Az irányított szolgáltatók és az irányított biztonsági szolgáltatók tekintetében jelentősnek minősülő biztonsági események

- az irányított szolgáltatás vagy az irányított biztonsági szolgáltatás több mint 30 percig egyáltalán nem áll rendelkezésre;

- az irányított szolgáltatás vagy az irányított biztonsági szolgáltatás a szolgáltatást igénybe vevő uniós felhasználók több mint 5 %-a vagy több mint 1 millió, a szolgáltatást igénybe vevő uniós felhasználó számára (amelyik szám kisebb) egy óránál hosszabb ideig korlátozottan áll rendelkezésre;

- az irányított szolgáltatás vagy az irányított biztonsági szolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;

- az irányított szolgáltatás vagy az irányított biztonsági szolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely az adott irányított szolgáltatást vagy az adott irányított biztonsági szolgáltatást igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy több mint 1 millió, az adott irányított szolgáltatást vagy az adott irányított biztonsági szolgáltatást igénybe vevő uniós felhasználót érint (amelyik szám kisebb).

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

Az online keresőprogramok szolgáltatói tekintetében jelentősnek minősülő biztonsági események

- az online keresőprogram az azt igénybe vevő uniós felhasználók több mint 5 %-a vagy több mint 1 millió, az adott online keresőprogramot igénybe vevő uniós felhasználó számára (amelyik szám kisebb) egyáltalán nem érhető el;

- az online keresőprogram korlátozott rendelkezésre állása az azt igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy a korlátozott rendelkezésre állás több mint 1 millió, az adott online keresőprogramot igénybe vevő uniós felhasználót érint (amelyik szám kisebb);

- az online keresőprogram rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;

- az online keresőprogram rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely az adott online keresőprogramot igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy több mint 1 millió, az adott online keresőprogramot igénybe vevő uniós felhasználót érint (amelyik szám kisebb).

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

A közösségimédia-szolgáltatási platformok szolgáltatói tekintetében jelentősnek minősülő biztonsági események

- a közösségimédia-szolgáltatási platform az azt igénybe vevő uniós felhasználók több mint 5 %-a vagy több mint 1 millió, az adott közösségimédia-szolgáltatási platformot igénybe vevő uniós felhasználó számára (amelyik szám kisebb) egyáltalán nem érhető el;

- a közösségimédia-szolgáltatási platform korlátozott rendelkezésre állása az azt igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy a korlátozott rendelkezésre állás több mint 1 millió, az adott közösségimédia-szolgáltatási platformot igénybe vevő uniós felhasználót érint (amelyik szám kisebb);

- a közösségimédia-szolgáltatási platform rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok sértetlensége, bizalmas jellege vagy hitelessége gyaníthatóan rosszindulatú tevékenység következtében sérül;

- a közösségimédia-szolgáltatási platform rendelkezésre bocsátásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely az adott közösségimédia-szolgáltatási platformot igénybe vevő uniós felhasználók több mint 5 %-át érinti, vagy több mint 1 millió, az adott közösségimédia-szolgáltatási platformot igénybe vevő uniós felhasználót érint (amelyik szám kisebb).

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

A bizalmi szolgáltatók tekintetében jelentősnek minősülő biztonsági események

- a bizalmi szolgáltatás több mint 20 percig egyáltalán nem áll rendelkezésre;

- a bizalmi szolgáltatás naptári hetek alapján számítva egy óránál hosszabb ideig nem érhető el a felhasználók vagy az igénybe vevő felek számára;

- a bizalmi szolgáltatás korlátozott rendelkezésre állása a szolgalátatás uniós felhasználóinak vagy uniós igénybe vevő feleinek több mint 1 %-át, vagy több mint 200 000 uniós felhasználóját vagy igénybe vevő uniós felét érinti (amelyik szám kisebb)

- fizikai hozzáférés történt egy olyan területhez, ahol hálózati és információs rendszerek találhatók, és amelyhez a hozzáférés csak a bizalmi szolgáltató megbízható személyzete számára engedélyezett, vagy az ilyen területhez való fizikai hozzáférés védelme sérült.

- bizalmi szolgáltatás nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely a bizalmi szolgáltatás uniós felhasználólóinak vagy uniós igénybe vevő feleinek több mint 0,1 %-át, vagy több mint 100 uniós felhasználóját vagy igénybe vevő felét érinti (amelyik szám kisebb).

A BIZOTTSÁG (EU) 2024/2690 VÉGREHAJTÁSI RENDELETE

Jelentős biztonsági események II.

(2) Az érintett szervezetek által vagy nevében végzett tervezett karbantartási műveletek miatti tervezett üzemszünetek, illetve az említett karbantartási műveletek tervezett következményei nem tekintendők jelentős biztonsági eseménynek. (CSIRT-nek jelenteni kell !!!)

(3) Az esemény által érintett felhasználók számának a 7. és 9–14. cikk alkalmazásában történő kiszámításakor az érintett szervezetnek figyelembe kell vennie az alábbiak mindegyikét:

a) azon ügyfelek száma, akik olyan szerződést kötöttek az érintett szervezettel, amely hozzáférést biztosít számukra az érintett szervezet hálózati és információs rendszereihez vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül hozzáférhető szolgáltatásokhoz;

b) az üzleti ügyfelekkel kapcsolatban álló olyan természetes és jogi személyek száma, akik az érintett szervezet hálózati és információs rendszereit vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül hozzáférhető szolgáltatásokat használják.

JELENTŐS ESEMÉNYEK BEJELENTÉSE

24 ÓRA

72 ÓRA

EGY HÓNAP

ELSŐ BEJELENTÉS

1. Az alapvető és fontos szervezetek számára elő kell írni, hogy amennyiben jelentős eseményről szereznek tudomást, indokolatlan késedelem nélkül és minden esetben 24 órán belül nyújtsanak be egy első bejelentést

Az első bejelentésnek csak azokat az információkat kell tartalmaznia, amelyek szükségesek ahhoz, hogy a CSIRT-ek vagy adott esetben az illetékes hatóságok értesüljenek a jelentős eseményről, és lehetővé tegyék az érintett szervezet számára, hogy szükség esetén segítséget kérjen. Ennek az első bejelentésnek adott esetben jeleznie kell, hogy feltételezhető-e, hogy a jelentős eseményt jogellenes vagy rosszhiszemű cselekmények okozták, és hogy valószínűsíthető-e, hogy az esemény határokon átnyúló hatásokkal jár.

BEJELENTÉS

A szervezetek az elektronikus információs rendszereikben bekövetkezett, illetve a tudomásukra jutott fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket és kiberbiztonsági incidenseket – beleértve az üzemeltetési kiberbiztonsági incidenst is – a nemzeti kiberbiztonsági incidenskezelő központ részére kötelesek haladéktalanul, a kormányrendeletben meghatározottak szerint bejelenteni.

Jelentős kiberbiztonsági incidensnek nem minősülő kiberbiztonsági incidenseket is bejelenthetik a nemzeti kiberbiztonsági incidenskezelő központ részére.

TOVÁBBI BEJELENTÉSEK

2. Az érintett szervezeteknek indokolatlan késedelem nélkül, és minden esetben a jelentős eseményről való tudomásszerzéstől számított 72 órán belül eseménybejelentést kell benyújtaniuk, különösen azzal a céllal, hogy frissítsék az első bejelentés keretében benyújtott információkat, és közöljék a jelentős esemény első értékelését, beleértve annak súlyosságát és hatását, valamint – amennyiben rendelkezésre állnak – a fertőzöttségi mutatókat(IoC).

3. Legkésőbb az eseménybejelentéstől számított egy hónapon belül zárójelentést kell benyújtani.
Abban az esetben, ha az esemény a zárójelentés benyújtásának időpontjában folyamatban van, a tagállamoknak biztosítaniuk kell, hogy az érintett szervezetek az adott időpontban az addig elért eredményekről szóló jelentést, a jelentős esemény általuk való kezelését követő egy hónapon belül pedig zárójelentést nyújtsanak be.

Jogkövetkezmények

(1) Ha a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat *nem teljesíti vagy nem tartja be*, a biztonsági hiányosságokat nem hárítja el, a megfeleléshez szükséges intézkedések meghozatalát elmulasztja, vagy a tevékenységet nem hagyja abba, a kiberbiztonsági hatóság:

a) Figyelmezteti a jogszabályokban foglalt biztonsági követelmények és az azokhoz kapcsolódó eljárási szabályok betartására, valamint határidő tűzésével felszólítja

b) kötelezheti a jogsértő magatartás megszüntetésére

c) a szervezetet felügyelő szervhez vagy a tulajdonosi joggyakorlóhoz fordulhat

d) d) jogosult kormányrendeletben meghatározottak szerint a szervezet költségére információbiztonsági felügyelőt kirendelni.

Jogkövetkezmények

(2) Ha az (1) bekezdés szerinti **intézkedések alkalmazása ellenére** az érintett szervezet (…) nem teljesíti vagy nem tartja be, a biztonsági hiányosságokat nem hárítja el (…) a kiberbiztonsági **hatóság az eset összes körülményének mérlegelésével** kormányrendeletben **meghatározott mértékű bírságot szabhat ki**, vagy más illetékes hatóságnál bírság kiszabását kezdeményezheti.

(7) A kiberbiztonsági hatóság a jogkövetkezmények alkalmazása során az **arányosság és a fokozatosság szempontjait figyelembe véve jár el**, szem előtt tartva a jogkövetkezmény hatékonyságát és visszatartó erejét.

(8) Ha a hatósági kötelezést a szervezet figyelmen kívül hagyja, vagy a kiberbiztonsági hatóság által javasolt védelmi intézkedéseket önhibájából nem teljesíti és **ezzel kiberbiztonsági incidens vagy kiberbiztonsági incidensközeli helyzet áll elő** a kiberbiztonsági hatóság (…) a helyzet bekövetkezésének **elhárítására fordított költségének megtérítésére kötelezheti.**

Jogkövetkezmények

(9) Ha az 1. § (1) bekezdés d) és e) pontja szerinti szervezet a jogszabályokban foglalt kiberbiztonsági követelményeket vagy az ehhez kapcsolódó eljárási szabályokat **nem teljesíti vagy nem tartja be**, **az SZTFH** az (1)–(4) bekezdésben **foglaltakon túl**

a) **jogosult** a szervezet tevékenységét engedélyező vagy felügyelő hatóság véleményének figyelembevételével **eltiltani az érintett szervezetet a biztonsági követelmények teljesülését közvetlenül veszélyeztető tevékenységtől**

Jogkövetkezmények

	A	B	C
	A jogszabálysértés megnevezése	A bírság legkisebb mértéke (forint)	A bírság legnagyobb mértéke (forint)
1.	az elektronikus információs rendszer biztonságáért felelős személy hatósági nyilvántartásba vételére irányuló kérelem benyújtásának elmulasztása	200.000	2.000.000
2.	információbiztonsági szabályzat hatósági nyilvántartásba vételére irányuló kérelem benyújtásának elmulasztása	200.000	2.000.000
3.	biztonsági osztályba sorolási kötelezettség elmulasztása	200.000	4.000.000
4.	az elektronikus információs rendszer biztonságáért felelős személy adatainak módosítására irányuló kérelem benyújtásának elmulasztása	200.000	2.000.000
5.	alapvető kiberhigiéniai gyakorlatok és kiberbiztonsági képzések szervezése vagy az ezeken való részvétel igazolásának elmulasztása	400.000	4.000.000
6.	eseménykezelő központtal való együttműködési kötelezettség elmulasztása	500.000	50.000.000
7.	a kiberbiztonsági hatóság vagy az eseménykezelő központ által elrendelt sérülékenységvizsgálati, illetve esemény kivizsgálási kötelezettség elmulasztása	500.000	50.000.000

Jogkövetkezmények

8.	a kiberbiztonsági hatóság által jóváhagyott sérülékenységkezelési terv szervezet általi végrehajtásának elmulasztása	200.000	10.000.000
9.	arányos biztonsági intézkedések bevezetésének és alkalmazásának elmulasztása	200.000	10.000.000
10.	a kiberbiztonsági incidens bejelentésének elmulasztása	500.000	5.000.000
11.	a szervezet által nyújtott szolgáltatás igénybe vevői, illetve az egyéb érintettek részére elrendelt tájékoztatási kötelezettség elmulasztása	2.000.000	20.000.000
12.	zárójelentés elkészítésnek elmulasztása, illetve nem megfelelő módon történő teljesítése	500.000	5.000.000
13.	a kiberbiztonsági hatóság végleges, végrehajtható határozatában foglalt kötelezésének nem teljesítése	1.000.000	50.000.000
14.	az információbiztonsági felügyelővel való együttműködés elmulasztása	1.000.000	40.000.000
15.	közvetítő szolgáltató együttműködési kötelezettségének megszegése	1.000.000	40.000.000

LEGFONTOSABB ÜZENET

1. NEM A HATÓSÁGI ELLENŐRZÉS MIATT KELL MEGFELELNI AZ ELŐÍRÁSOKNAK

2. NEM A BÜNTETÉS ELKERÜLÉSE MIATT KELL AZ INCIDENST BEJELENTENI

3. A BEJELENTÉST MEG LEHET TENNI E-MAILBEN ÉS TELEFONON IS

INCIDENSBEJELENTÉS

+36 (1) 336 4833

+36 (30) 344 0704

CSIRT@nki.gov.hu

nki.gov.hu

KÖSZÖNÖM A FIGYELMET !!!