Információvédelem menedzselése
LXXXIV. Szakmai Fórum

2019. január 16.

Bejelentés-köteles szolgáltatók kötelezettségei a NIS irányelv tükrében

Dr. Bonnyai Tünde PhD

Kinek/minek a szempontjából?

gazdasági tevékenységek
társadalmi tevékenységek
belső piac működése
pénzügyi veszteségek
felhasználói bizalom

Kire/mire gyakorol hatást?

szolgáltató
felhasználó
nemzetgazdaság
államigazgatás
közbiztonság
EU belső piac

Mekkora hatást gyakorol?

belső
lokális
regionális
nemzeti
közösségi
globális

Az Európai Parlament és a Tanács (EU) **2016/1148 irányelve** (2016. július 6.) **a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről** (NISD)

A Bizottság (EU) **2017/179 végrehajtási határozat**a (2017. február 1.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 európai parlamenti és tanácsi irányelv 11. cikkének (5) bekezdése értelmében **az együttműködési csoport működéséhez szükséges eljárásrend megállapításáról**

A Bizottság (EU) **2018/151 végrehajtási rendelet**e (2018. január 30.) a hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából **a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek** pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok **meghatározásáról**

CÉLKITŰZÉSEK

MIT?

Biztonsági szint növelése

Kockázatkezelés kultúrájának előmozdítása

Kibertámadásokkal szembeni védekező és ellenálló képesség fejlesztése

Nélkülözhetetlen szolgáltatások védelme

MIVEL?

Kockázatokkal arányos biztonsági intézkedések megtétele

Hatósági felügyelet erősítése

Súlyos biztonsági események bejelentése / elemzése

HOGYAN?

1. Nemzeti kiberbiztonsági képességek javítása
2. Stratégiai célkitűzések megalkotása és végrehajtása
3. Kockázatmenedzsment fejlesztése
4. Hatósági szerepkörök pontosítása – szereplők azonosítása
5. Hiányosságok pótlását szolgáló utasítások kiadása…

…útján

HOGYAN?

Nemzeti kiberbiztonsági képességek javítása
Stratégiai célkitűzések megalkotása és végrehajtása

- STRUKTÚRA
- FELELŐSSÉGI KÖRÖK
- EGYÜTTMŰKÖDÉS
- FELKÉSZÜLTSÉG
- KOCKÁZATELEMZÉS
- REAGÁLÓ KÉPESSÉG
- OKTATÁS-KÉPZÉS
- TUDATOSÍTÁS
- KUTATÁS-FEJLESZTÉS

HOGYAN?

Kockázatmenedzsment fejlesztése

BIZTONSÁGI ESEMÉNY DEFINIÁLÁSA

KOCKÁZATOK AZONOSÍTÁSA

KOCKÁZATOK ÉRTÉKELÉSE

MEGELŐZŐ INTÉZKEDÉSEK

FELDERÍTÉS & ÉSZLELÉS

BIZTONSÁGI ESEMÉNY KEZELÉSE

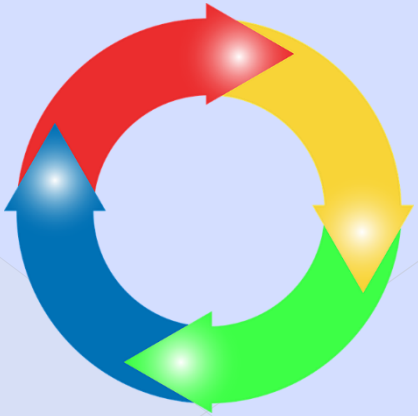
HATÁSOK MÉRSÉKLÉSE

KÖVETKEZMÉNYEK KEZELÉSE

KOCKÁZATOK AZONOSÍTÁSA

KOCKÁZAT

minden olyan ésszerűen azonosítható körülmény vagy esemény, amely kedvezőtlen hatást gyakorolhat a hálózati és információs rendszerek biztonságára



HOGYAN?

Hatósági szerepkörök pontosítása – szereplők azonosítása
Hiányosságok pótlását szolgáló utasítások kiadása

(TAG)ÁLLAMI GARANCIÁK

Hatóság(ok)

CSIRT-ek

Egyedüli nemzeti kapcsolattartó pont

Nemzeti struktúra

Végrehajtható stratégia

+EU Együttműködési Csoport

Hatáskör & felügyelet

Együttműködés (PPP) fejlesztése

Minimumkövetelmények

Szakmai támogatás & szankció

Információcsere

ÜGYFÉLKÖR

Alapvető szolgáltatást nyújtó szereplők

Digitális szolgáltatást nyújtók

BIZTONSÁG
INTEGRITÁS
ELLENÁLLÓ KÉPESSÉG

szavatolása fejlesztése

NIS (44)

„Az információs rendszerek biztonságának biztosítása nagymértékben az alapvető szolgáltatást nyújtó szereplők és a digitális szolgáltatók felelőssége.”

CÉLCSOPORTOK

Alapvető szolgáltatást nyújtó szereplők

Olyan közjogi vagy magánjogi szervezet, amely

- ✓ **kritikus társadalmi** és/vagy **gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt,**
- ✓ az adott **szolgáltatás nyújtása hálózati és információs rendszerektől függ**, és
- ✓ az említett **szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában,** valamint
- ✓ **beletartozik az alábbi ágazatok valamelyikébe:**
  - Energia
  - Közlekedés
  - Banki szolgáltatások
  - Pénzügyi piaci infrastruktúrák
  - Egészségügy
  - Ivóvízellátás és –elosztás
  - Digitális infrastruktúra

Digitális szolgáltatást nyújtók

Minden olyan jogi személy, amely az alábbi típusokba sorolható digitális szolgáltatást nyújt:

- ✓ online **piactér**,
- ✓ online **keresőprogram**,
- ✓ **felhőlapú** számítástechnikai **szolgáltatás**.

NEM kell alkalmazni:

- azokra a **vállalkozás**okra amelyek olyan, **nyilvános hírközlő hálózatokat üzemeltet**nek vagy **nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújt**anak, amelyek **különös biztonsági és integritási követelmények*** hatálya alá tartoznak;
- olyan **bizalmi szolgáltatók**ra, amelyek **külön rendeletben megállapított biztonsági követelmények**** hatálya alá tartoznak;
- digitális szolgáltatást nyújtó **mikro- és kisvállalkozások**ra;
- **online szolgáltatások**ra, amelyek csupán **köztes lépéseket jelentenek** olyan harmadik fél által nyújtott szolgáltatások előtt, amelyek keretében a szerződések végleges megkötésére sor kerülhet;
- **hardvergyártók és a szoftverfejlesztők nem minősülnek** alapvető szolgáltatást nyújtó szereplőknek vagy digitális szolgáltatóknak

* 2002/21/EK irányelv ** 910/2014/EU irányelv

Digitális szolgáltatást nyújtók

Online piactér

fogyasztók és a kereskedők online adás-vételi és/vagy szolgáltatási szerződéseket kötnek, amely szerződések végpontjai a piacterek (kivétel pl. arukereso.hu; de pl. ide tartozik a GooglePlay, a B2C-k, stb.)

Online keresőprogram

a felhasználók egy adott kulcsszó alapján elvben minden webhelyen keresést hajthatnak végre, és ennek eredményeként hivatkozásokat érnek el (kivétel meghatározott webhelyre korlátozott keresőfunkciók; és pl. arukereso.hu)

Felhő alapú számítástechnikai szolgáltatás

olyan szolgáltatások, amelyek megosztható (több olyan felhasználó számára biztosított, akik közös hozzáféréssel rendelkeznek, de a feldolgozás külön történik) számítástechnikai erőforrások (pl.: hálózat, szerver) méretezhető és rugalmas (keresletnek megfelelően nyújtott)pooljához engednek hozzáférést

CÉLCSOPORTOK
NIS ÁLTAL BEVEZETETT **KÖTELEZETTSÉGEI**

BIZTONSÁGI ÉS BEJELENTÉSI KÖVETELMÉNYEK TELJESÍTÉSE

KOCKÁZATMENEDZSMENT kialakítása

kötelező kockázatértékelés, kockázatok számszerűsítése, elemző-értékelő eljárások alkalmazása, humán-erőforrás szempontok érvényesítése

intézkedések megtétele a valós kockázatokkal arányos, az adott hálózati és információs rendszer ellenállóképességének növelése érdekében

BIZTONSÁGI ESEMÉNY bejelentése

indokolatlan késedelem nélkül bejelentik a szolgáltatás folytonosságára jelentős hatást gyakorló biztonsági eseményeket

KÖVETELMÉNYEK

Kockázat alapú megközelítés alkalmazása

Kockázatok azonosítása, **súlyosságuk számszerűsítése**

A rendszer szisztematikus irányítása keretében végzett kockázatelemzés során tett intézkedések

kritikus létesítményeket fenyegető **veszélyek azonosítása**
működésre gyakorolt **potenciális hatások** felmérése
veszélyek eredményes csökkentésének lehetőségei

Folytonosság érdekében **megelőző és a hatások csökkentésére irányuló** intézkedések

Felmerülő **kockázatoknak megfelelő biztonsági szint folyamatos garantálása**

arányos és megfelelő műszaki és szervezési intézkedések

KÖVETELMÉNYEK

arányos és megfelelő műszaki és szervezési intézkedések

fizikai és környezeti biztonság, ellátás biztonsága, hálózati és információs rendszerek integritása rendszerekhez való hozzáférés ellenőrzése	**rendszerek és létesítmények biztonsága**
folytonosságot szolgáló stratégiai és vészhelyzeti tervek katasztrófaelhárítási képességek	**üzletmenet-folytonosság-menedzsment**
monitoringra és a naplózásra vonatkozó előírások, vészhelyzeti tervek gyakorlása, hálózati és információs rendszerek tesztelése, biztonsági értékelések és a megfelelés monitoringja	**monitoring, audit és tesztelés**
készségek kezelése, fejlesztése tudatosság növelése	**humánerő-forrás**

KÖVETELMÉNYEK

Biztonsági események hatásaira vonatkozó **paraméterek**

Biztonsági események késedelem nélküli **bejelentése**

Bejelentési kötelezettséggel kapcsolatos intézkedések

biztonsági esemény észlelése
biztonsági esemény bejelentése
eseményről való tájékoztatás
rendszer hiányosságainak, sebezhető pontjainak feltárása
eljárásoknak megfelelő reagálás, esemény értékelése, dokumentálása

EU VHR. 3. cikk

a biztonsági esemény által érintett felhasználók száma
biztonsági esemény időtartama
biztonsági esemény által érintett terület földrajzi lehatárolása
működés zavarának mértéke
gazdasági és társadalmi tevékenységekre gyakorolt hatás mértéke

*Annak érdekében, hogy az illetékes hatóságok értesülhessenek a potenciális új kockázatokról, a **digitális szolgáltatókat arra kell ösztönözni, hogy önkéntes alapon jelentsenek be minden olyan eseményt, amelyek számukra addig ismeretlen jellemzőkkel bírtak**, legyenek azok új sérülékenységet kihasználó módszerek, támadási vektorok vagy támadó felek, sebezhető pontok vagy fenyegetések. NIS VHR (11)*

HAZAI SZABÁLYOZÁS (BEJELENTÉS-KÖTELES SZOLGÁLTATÓK)

2001. CVIII. Eker. tv.:

definíciós háttér és különleges szabályok

- Nyilvántartás vezetése
- Követelmények teljesítésének ellenőrzése
- Hatósági eljárás, szankcionálás

- **Regisztráció**
- Előírt **követelmények teljesítése**
- Biztonsági esemény **bejelentése**
- Hatósági **döntések végrehajtása**

KIVÉTELEK

- **Mikro- és kisvállalkozások 50 főnél kevesebb foglalkoztatott**al bír **és éves nettó árbevétele vagy mérlegfőösszege max. 10 millió €**
- **Kijelölt** nemzeti vagy európai **létfontosságú rendszerelemek**
- **Ibtv.** személyi **hatálya** alá tartozók

270/2018. (XII. 20.) kormányrendelet:

részletszabályok

- Hatóság feladatai, szolgáltatói biztonsági követelmények
- Biztonsági esemény és bejelentésével kapcsolatos szabályok
- Jogkövetkezmények

Gondoskodik *azon megfelelő* ***dokumentumok rendelkezésre állásáról****, amelyek* ***lehetővé teszik*** *a rendszerek és létesítmények biztonsága érdekében* ***alkalmazott biztonsági elemek megfelelőségének*** *hatóság általi* ***ellenőrzését***

A bejelentés-köteles szolgáltató

REGISZTRÁL

hatóság honlapján közétett formában, tartalommal
(gazdasági társaság elnevezése, székhelye, cégjegyzékszáma, elektronikus kapcsolattartási adatai, nyújtott bejelentés-köteles szolgáltatás típusa)

EGYÜTTMŰKÖDIK

különösen a hatóság által végzett ellenőrzések során, kiadott döntések végrehajtása tekintetében, biztonsági esemény kezelése és kivizsgálása időszakában,
egyéb érintettre is vonatkozó kötelezettség

BEJELENT

biztonsági eseményeket, amelyek hatást gyakorolnak a szolgáltatás nyújtására (haladéktalanul)
tevékenység megszűnése, létfontosságúvá történő kijelölés, egyéb változások (8 nap)

BEJELENT

biztonsági eseményeket, amelyek hatást gyakorolnak a szolgáltatás nyújtására (haladéktalanul)

1. A **hatás jelentőségének megállapítása**kor a már említett **EU végrehajtási rendelet 3. cikk** szerinti **paraméterek**et kell figyelembe venni
2. **Csak akkor kell bejelenteni**, ha a bejelentés-köteles szolgáltató számára elérhetők azok az információk, amelyek alapján a **paraméterek figyelembevételével ki tudja értékelni** a biztonsági esemény **hatását**
3. **Önkéntes alapon bejelenthetnek** minden olyan eseményt, amelyek addig ismeretlen jellemzőkkel bírtak (sérülékenységet kihasználó új módszereket, sebezhető pontokat, fenyegetéseket, stb.)
4. **Kormányzati eseménykezelő központ (GovCert) részére** kell bejelenteni
5. **Elsődlegesen elektronikus úton**, ha nem megoldható bármely más módon
6. **Tartalma legalább**: a biztonsági esemény **rövid leírása**, státusza, a **zavar mértéke**, az esemény kezelésére kijelölt **kapcsolattartó** elérhetőségei, az esemény **hatását meghatározó szempontok**

Hatóság

Nemzetbiztonsági Szakszolgálat

(hatóság, GovCert, egyedüli kapcsolattartó)

Biztonsági esemény (Ibtv. 1. § 9.) **+ 41a. (!!)**

__nem kívánt__ vagy __nem várt egyedi__ esemény, amely az elektronikus információs rendszerben __kedvezőtlen változást__ vagy egy előzőleg __ismeretlen helyzetet idéz elő__, és amelynek hatására a __hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész__, illetve __megsérül__

NYILVÁNTARTÁS

- a **szolgáltató** regisztrációja és adatbejelentései alapján

KAPCSOLATTARTÁS

- **szolgáltatókkal,** rendvédelmi szervekkel, EU intézményekkel és tagállamokkal, Nemzeti Adatvédelmi és Információszabadság Hatósággal

TÁJÉKOZTATÁS

- **szükség szerint** a nyilvánosságot, a bekövetkezett **biztonsági eseményekről**

HATÓSÁGI ELLENŐRZÉS

- **szolgáltatók** kötelezettségeinek teljesítését ellenőrzi

HATÓSÁGI ELJÁRÁS

- információbiztonsági **követelmények nem teljesülése esetén indítja**
- szolgáltatónál helyszíni ellenőrzés tarthat

MIRE KÖTELEZHET ENGEM, MINT DIGITÁLIS SZOLGÁLTATÓT A HATÓSÁG?

HATÁRIDŐ MEGÁLLAPÍTÁSÁVAL

- ✓ **bocsássam rendelkezésre** az információs rendszereim biztonságának megállapításához szükséges adatokat, dokumentumokat,
- ✓ gondoskodjak a kockázatoknak **megfelelő biztonsági szint biztosítás**áról,
- ✓ intézkedjek a **biztonsági esemény megelőzés**ére, **bejelentés**ére, **kezelés**ére,
- ✓ **teljesítsem** a jogszabályban meghatározott **kötelezettségeimet**,
- ✓ **szüntessem meg** a tapasztalt **hiányosságokat,** amelyeket ellenőrzés keretében, vagy biztonsági eseményt követően feltártak,,
- ✓ **azonnali intézkedéseket tegyek**, ha a hiányosság, mulasztás, vagy a megsértett biztonsági követelmény **súlyos biztonsági esemény bekövetkeztével fenyeget,**

MIRE KÖTELEZHET ENGEM, MINT DIGITÁLIS SZOLGÁLTATÓT A HATÓSÁG?

- ✓ **elhárításra javasolt intézkedéseket** foganatosítsak, amelyeket a biztonsági eseményt követő vizsgálat eredményeként javasol,
- ✓ **további károkozás megelőzése érdekében** további **intézkedéseket** tegyek, amelyeket a vizsgálat eredményeként javasol,
- ✓ **tájékoztassam** a **nyilvánosságot** a bekövetkezett biztonsági esemény kapcsán, ha az egy másik biztonsági esemény megelőzése miatt szükség van, vagy ha a bejelentés a közérdeket szolgálja.

MIKOR?

Ha a szolgáltató **nem teljesíti** a hatósági döntés tartalmát

MIÉRT?

Regisztráció elmulasztása
Adatváltozás bejelentésének elmulasztása
Kockázatelemzés elmulasztása*
Biztonsági **intézkedés bevezetés/alkalmazás** elmulasztása
Kockázatelemzés és intézkedések **felülvizsgálatának** elmulasztása
Biztonsági esemény **bejelentésének** elmulasztása
Hatóság döntésének nem teljesítése

BÍRSÁG

Kockázatelemzés elmulasztása*

- ✓ **A <u>korábbi kormányrendelet</u>** tartalmazott olyan kötelezettséget, hogy **a szolgáltató kockázatelemzést készít**sen**, de ez <u>most nem része a szabályozásnak</u>**

A kockázatelemzés készítése kiterjedt:

- ✓ a hálózati és információs rendszerek és létesítmények biztonságára,
- ✓ a biztonsági események kezelésére és
- ✓ az üzletmenet folytonosság biztosítására.

- ✓ A kidolgozott kockázatelemzés alapján a kockázatokkal arányos biztonsági intézkedések bevezetése és alkalmazása volt kötelező
- ✓ A kockázatelemzést és a biztonsági intézkedéseket bekövetkezett biztonsági eseményt követően haladéktalanul, de legalább évente kellett volna célszerűen felülvizsgálni.

DE MIVEL SZEMBEN VÉDJEM?

„tipikus fenyegetettségek”

- ✓ túlterheléses támadás (DoS, DDoS)
- ✓ adathalászat, adatvesztés
- ✓ identitás lopás
- ✓ fizető felület sérülékenysége
- ✓ SQL injection
- ✓ publikált sérülékenységek kihasználása
- ✓ social engineering
- ✓ belső támadások

HASZNOS

- ✓ ENISA - https://www.enisa.europa.eu/
- ✓ jó gyakorlatok, szabványok használata (COBIT, ISO 27000 szabványcsalád, ITIL)
- ✓ naprakész jogosultságkezelés
- ✓ naprakész (biztonsági) frissítések
- ✓ megbízható, releváns fejlesztők alkalmazása
- ✓ Ingyenes / ismeretlen eredetű modul-adatbázis kezelő rendszerek kerülése
- ✓ biztonsági mentések, auditálás, stb…

Köszönöm
a megtisztelő figyelmet!