With integrity, you have nothing to fear, since you have nothing to hide. With integrity, you will do the right thing, so you will have no guilt.
- Hilary Hinton "Zig" Ziglar*

Adatvédelmi incidens fogalma
Miben más az adatvédelmi és a biztonsági incidens?

Dravecz Tibor
INTEGRITY Kft.

2019. október 8.

Esemény és incidens

Először is hangsúlyozzuk, hogy a

(BIZTONSÁGI) **ESEMÉNY és INCIDENS fogalma**

alapvetően eltérő - az INCIDENS szűkebb fogalom (nagyságrendekkel több esemény történik, mint incidens).

"**An EVENT is any observable occurrence in a system or network**" NIST.SP.800-61r2[1]

"Adverse events [kedvezőtlen/kárt okozó esemény] are events with a negative consequence" NIST.SP.800-61r2

[1] National Institute of Standards and Technology U.S. Department of Commerce (NIST): Security Incident Handling Guide

Informatikai biztonsági incidens

Informatikai biztonsági incidens (Computer Security Incident) fogalma alatt az informatikában valami olyasmit értünk, hogy a megszokott vagy elvárt biztonság folyamata megszakad, veszélyhelyzet teremtődött vagy kár keletkezett

'Tankönyvi' definíciónak is tekinthető a **NIST**[2,3]-é: **"A COMPUTER SECURITY INCIDENT is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." NIST.SP.800-61r2 — Ez valójában metadefiníció!**

A NIST definíció **RELATÍV** definíció, a NIST szabványt követő szervezeteknek, vállalkozásoknak ennek alapján kellene alkotni ún. szervezeti definíciót (organisation definition) a biztonsági incidensre.

Az **ISO 27000** definíció: "An information security incident is made up of one or more unwanted or unexpected information security events that could possibly compromise the security of information and weaken or impair business operations." (Valójában az ISO 27000-es sorozatban többféle definíció is van erre).

[2] Azok is de facto szabványnak tekintik, akik számára nem de jure szabvány, illetve általában az informatikában mérvadónak és iránymutatónak tekintik, széles körben követik is a National Institute of Standards and Technology U.S. Department of Commerce (NIST) által kiadott Computer Security Incident Handling Guide című dokumentumot.
[3] Sok másféle de facto és de jure definíció ismert; ajánlások, szabványok, jogszabályok különféle definíciókat vezettek be, az itt tárgyalt gondolatok többé-kevésbe többségükre érvényesek.

Elérhetőség (availibily) és biztonság (security)

Régebben a **számítástechnikában** jellemzően elkülönítve kezelték az **ELÉRHETŐSÉG**et **(RENDELKEZÉSRE-ÁLLÁS**t**)** a **BIZTONSÁG**tól, tipikusan nem a biztonság részeként.

Események és incidensek tekintetében a rendelkezésre-állási események kezelése sok esetben el is tér, illetve elkülönül.

Manapság azonban az **elérhetőség** (rendelkezésre-állás) fogalmát, mint a biztonság egy kategóriáját tekintjük, a legfontosabb biztonsági kategóriák,

az ún. CIA triád részeként:

- confidentality,
- integrity,
- **availability (elérhetőség)**.

És most térjünk rá a biztonsági és az adatvédelmi incidens viszonyára!

Adatvédelmi incidens jogszabályi definíció

"„**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**"

- Általános adatvédelmi rendelet, 4. cikk 12. (Fogalommeghatározások)

"'**personal data breach**' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;"

- General Data Protection Regulation, REGULATION (EU) 2016/679 (12) Article 4 (Definitions)

"**adatvédelmi incidens**: az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi" - Infotörvény[4]

[4]2018. évi XXXVIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról, 2. § (10) http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK18117.pdf

Adatvédelmi incidens fogalma

Miben más, mint az informatikai biztonsági incidens:

- jogszabályi definíció;
- abszolút (azaz nem relatív) fogalom,
  - illetve mégis beleérthető egy kis relativitás, mert az "„adatvédelmi incidens”: a biztonság olyan sérülése …"

Eshetőség versus bekövetkezés:

- 'eredmény(ezés)' nélkül még nincs adatvédelmi incidens,
  - azaz fenyegetettség, veszély,
  - szabályok megszegése,
  - (az elfogadott vagy elfogadható gyakorlat) megsértése még önmagában nem jelenthet adatvédelmi incidenst;
- a rendelkezésre-állás kérdése pedig valamelyest szürke zónának tekinthető.

A biztonsági incidens relatív voltának következményei

Az említett NIST definíció szerint súlyos következménnyel járó biztonsági esemény is lehet nem incidens.

Példa: Az adott szervezetben a biztonság teljesen szabályozatlan, és ez per definíció kizárja a biztonsági incidens lehetőségét :-(

Személyes adatokat érintő esemény, mely következtében emberek halnak meg, még nem feltétlenül jelent adatvédelmi incidenst

Nem szükségképpen adatvédemi incidens a következő (nagyon sarkított, de nem abszurd példa): meghibásodás következtében személyes adatok, történetesen fontos egészségügyi adatok elérhetősége átmenetileg lassult, akadozott (vagy akár átmenetileg elérhetetlenné vált, bár erre már kényszeredve ráfogható, hogy átmenetileg személyes adat 'elveszett'), mely esemény számos ember halálához vezetett (pl. járványügyi vészhelyzetben nem vagy csak késbe lehetett meghozni szükséges óvintézkedéseket).[5]

(Arról nem szóltunk, hogy adatvédelmi felügyeleti szerv minek tekintené, csupán azt mondtuk, hogy jogszabály szerint ilyen esemény nem szükségképpen adatvédelmi incidens, és önmagában biztos nem az.)

[5] A W29-es cikk alapján létrehozott munkacsoport egy hasonló példát hozott fel, de más következtetést tett közzé róla. Különbség a részletekből, illetve abból adódik, hogy 'józan ész' szerinti szubjektív értelmezés vagy a rendelet szövegének objektív jelentéstartalma-e a kiindulópont.

Tartalom