HADMÉRNÖK

X. Évfolyam 4. szám - 2015. december

ORBÓK Ákos
orbok.akos@uni-nke.hu

RÖVID ÁTTEKINTÉS A NEMZETI KIBERVÉDELMI INTÉZET MEGALAKULÁSÁRÓL, MŰKÖDÉSÉRŐL ÉS ELŐZMÉNYEIRŐL

Absztrakt

Magyarország kibervédelme 2015. október 1-én gyökeresen átalakult a Nemzeti Kibervédelmi Intézet (NKI), azaz az állami és önkormányzati szervek elektronikus információs rendszerei védelmét támogató szervezet megalakulásával. A korábbi heterogén struktúrát egy átlátható hierarchia váltja fel. Az új szervezet feladatköre több funkcióval is bővült, amelyek az állami szereplők működését támogatják és felügyelik.

Hungary's cyber defense completely transformed on October 1, 2015. The National Cyber Defence Institute (NKI), to support the protection of electronic information systems of state and municipal agencies. The previous heterogeneous structure was replaced by a transparent hierarchy. The new organization's responsibilities expanded even more features to support and supervise the functioning of the state actors.

Kulcsszavak: *Nemzeti Kibervédelmi Intézet, új struktúra ~ National Cyber Defence Institute, the new structure*

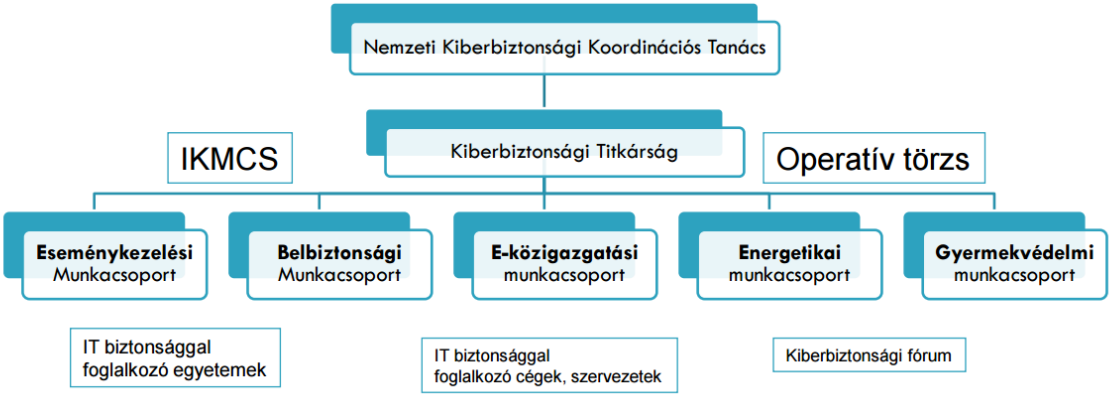
BEVEZETÉS

Hazánkban a kiberbiztonság állami szervezeti keretei néhány éves múltra tekintenek vissza. A 2015 őszén megalakult Nemzeti Kibervédelmi Intézet (NKEI), amely szervezet sajtótájékoztató keretében mutatta be leendő felépítését, feladatait és tervezett működését 2015. október 28-án.

Mielőtt azonban mindezeket bemutatnánk célszerű a hazai kiberbiztonságot meghatározó és azt szabályozó jogszabályokat időrendi sorrendben áttekinteni, hiszen ezek a jelenleg érvényben lévő szabályozást megelőzően is komoly kihatással voltak a magyarországi információbiztonságra. Ezek a jogszabályok a következőek voltak:

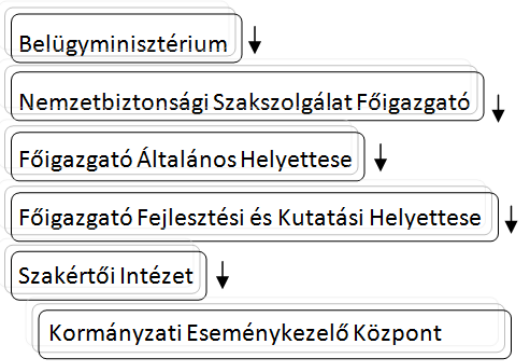
- 65/2013. (III.8.) Korm. rendelet A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
- 1139/2013. (III.21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 2013. évi L. (IV.15.) törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról
- 233/2013. (VI.30.) Korm. rendelet Az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről.
- 301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról

2013. március 21-én elfogadott kormányhatározatot követően (Magyarország Nemzeti Kiberbiztonsági Stratégiája), 2013. április 15-én az Országgyűlés elfogadta az állami és önkormányzati szervezetek elektronikus információbiztonságáról szóló törvényt, amelynek alapján létrejött a magyarországi kibervédelmi szervezetrendszer. Ennek célja - a kibertér biztonsági környezetének elemzése alapján - azon nemzeti célok, stratégiai irányok, feladatok és átfogó kormányzati eszközök meghatározása, amelyek alapján az ország érvényesíteni tudja nemzeti érdekeit a kibertérben. Ezt a szervezetrendszert mutatja be az 1. ábra.



1. ábra: A hazai kiberbiztonság szervezeti keretei 2015 júniusa előtt
(Forrás: Gyebrovszki Tamás: GovCERT bemutatkozás 2014. március 26.)[2]

A szervezetrendszeren belül megalakultak különböző munkacsoportok, együttműködési fórumok, a kiberbiztonsági koordinációs tanács, a Kormányzati Eseménykezelő Központ (GovCERT). Megalakultak továbbá az ágazati CERT-ek, a Nemzeti Elektronikus Információbiztonsági Hatóság, valamint a szakhatósági feladatokat, gyakorlatilag a sérülékenység vizsgálatokat ellátó, a Nemzeti Biztonsági Felügyelet szervezeti keretein belül működő Cyber Defence Management Authority (CDMA csoport). [1]



2. ábra: A GovCERT helye a belügyminisztériumban 2015. október 1. előtt

JELENLEGI SZERVEZEZETI FELÉPÍTÉS ÉS MŰKÖDÉS

Az állami és önkormányzati szervezetek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításának eredményeként 2015. október 1-jétől megalakult a Nemzeti Kibervédelmi Intézet (NKI), amelynek működését, felépítését mutatta be Dr. Bencsik Balázs az intézmény vezetője 2015. október 28-i sajtótájékoztatóján. A korábbi heterogén struktúra, amely a feladatokat különböző intézmények között osztotta szét nem volt egységes rendszerbe szervezve így a hatékonysága is korlátozott volt.

A korábbi, széttagolt struktúra a következő volt:

- hatósági feladatok: Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH);
- szakhatóság: Nemzeti Biztonsági Felügyelet CDMA;
- informatikai biztonsági eseménykezelés: NBSZ GovCERT;
- Kiberbiztonsági Koordinációs Tanács.

Ugyanakkor az új struktúra egy intézményben egyesíti az eseménykezelő központot, a felügyelő hatóságot és a tanácsadó funkciót. Mindezeket a Belügyminisztérium felügyeli. A kiberbiztonsági struktúra egy átlátható hierarchikus rendszerré alakult a változásokat követően (3. ábra).

Az intézmények védelmét egy biztonsági életciklus bevezetésével kívánják hatékonyabbá tenni. Az életciklus egyes állomásaiért az intézet különböző jogkörrel felruházott részei felelősek. Négy fő részre lehet bontani az életciklust: tervezés, szabályozás, fenntartás-felügyelet, incidensek elhárítása. A 4. ábrán jól látható hogyan kapcsolódnak a különböző feladatok az egyes ciklusokhoz és az intézet különböző részeihez.

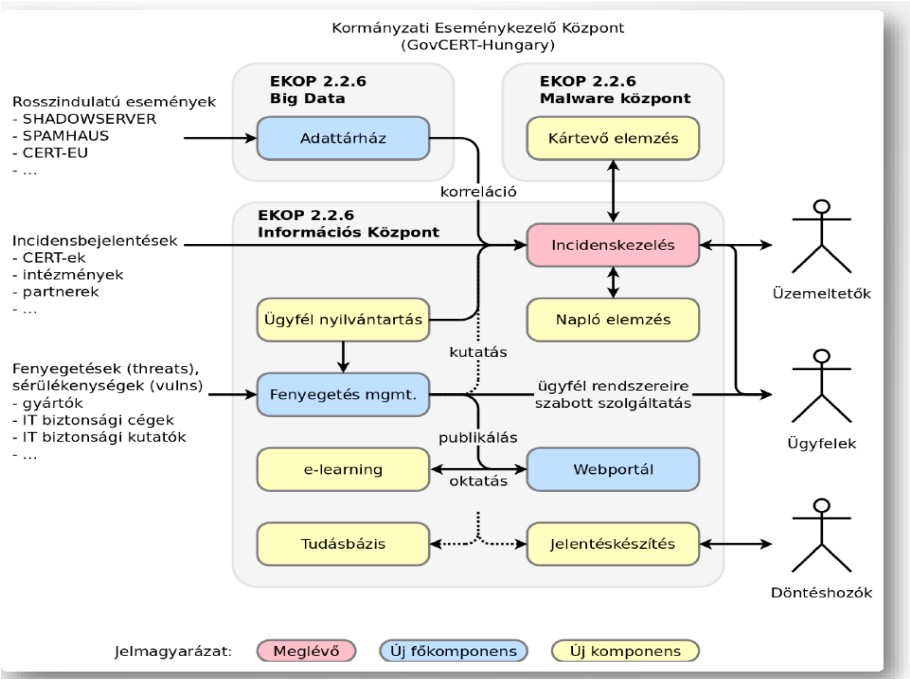
A majdnem egy hónapja működő intézménynek máris kezelnie kellett egy támadást a kormányzati rendszerek ellen. 2015 harmadik negyedévében észlelt rosszindulatú tevékenységek, amelyek a kormányzati rendszerek ellen irányultak a 4. ábrán látható arányban jelentkeztek.

3. ábra: (Forrás: Dr. Bencsik Balázs prezentációja 2015.okt.28.)

A struktúra átalakulása egyben egy paradigmaváltással is együtt járt. Az intézmények védelme egy meghatározott életciklus mentén valósul meg. A NEIH feladatköre megmaradt, kibővült és integrálódott a kormányzati IT biztonsági életciklusba. (3. ábra) Az ellenőrzési és a hatósági feladatokat egyesítve hatékonyabban képes detektálni a sérülékeny pontokat az egyes intézmények működésében. Részben hozzá tartozik a biztonsági tervezés és a sérülékenység vizsgálat, valamint a biztonsági szabályozások meghatározása az előbbiekből következően a védelem kialakítása.

4. ábra: (Forrás: Dr. Bencsik Balázs prezentációja 2015.okt.28.)

A kormányzati eseménykezelő központ (GovCERT-Hungary) tevékenysége is kibővült. Az eddig alapvetően a gyors reagálású incidenskezelés mellett 2015. október 1-től más feladatokkal is ellát majd a központ. A feladatok jellemzően a különböző kormányzati kliensek felügyeletéből és az incidensek elemzéséből, valamint a sérülékenységek feltárásából állnak. A feladatbővítés magában foglalja a kliensek felkészítését is, amelyet tudatosítással, oktatással, kutatásokkal kívánnak elérni.



5. ábra: A GovCERT belső folyamatai
(Forrás: Dr. Bencsik Balázs prezentációja 2015. okt. 28.)

A Nemzeti Kibervédelmi Intézet felhasználja a már – többek között a GovCERT-Hungary-nél – meglévő nemzetközi kapcsolatokat. Ennek keretében tovább építi a számos külföldi kibervédelmi szervezettel, CERT-ekkel és nemzetközi kibervédelmi szervezettel (European Network and Information Security Agency - ENISA, Forum of Incident Response and Security Teams - FIRST, Trusted Introducer - TI, International Watch and Warning Network - IWWN, European Government CERTs Group - EGC) már fennálló szakmai kapcsolatait.

A hazai állami elektronikus információs rendszerek biztonsága az elmúlt években határozott fejlődésnek indult, azonban a teljes körű biztonsági szint eléréséhez még sok a tennivaló. A kielégítő kiberbiztonság ugyanis nem teremthető meg pusztán a szervezetrendszer kialakítása és az általa működtetett biztonsági rendszerek fejlesztésével, üzemeltetésével. A már meglévő és biztonságilag hiányos rendszereknél következetesen végig kell vinni az Ibtv.-ben megfogalmazott, a biztonsági szint emelését előíró folyamatokat, az újonnan fejlesztendő rendszereknél pedig kiemelt figyelmet és megfelelő pénzügyi erőforrást kell fordítani az elektronikus információbiztonság kialakítására.

Emellett minden szinten – vezetői, fejlesztői, üzemeltetői, felhasználói stb. – növelni kell az információvédelem tudatosítását, ugyanis kizárólag technikai eszközökkel nem, vagy csak irreálisan magas költségekkel valósítható meg az állami rendszerek védelme. A biztonságtudatos magatartás és a biztonsági technikai fejlesztések, valamint a hozzájuk kapcsolódó szervezetrendszer – ezen belül a Nemzeti Kibervédelmi Intézet – hatékony működtetése együttesen szükséges a megfelelő kiberbiztonsági szint biztosításához.

Felhasznált irodalom:

[1] http://www.kormany.hu/hu/belugyminiszterium/rendeszeti-allamtitkarsag/hirek/megalakul-a-nemzeti-kibervedelmi-intezet (2015. nov. 20.)

[2] Gyebrovszki Tamás: GovCERT bemutatkozás, Nemzetbiztonsági Szakszolgálat 2014. március 26. http://archive.ivsz.hu/hu/_/media/Files/mcs/ICT-biztonsag/worksop20140326/GovCERT_el%23U0151ad%23U00e1s_ICT%20Biztons%23U00e1g%20workshop2.pdf (2015. nov. 20.)