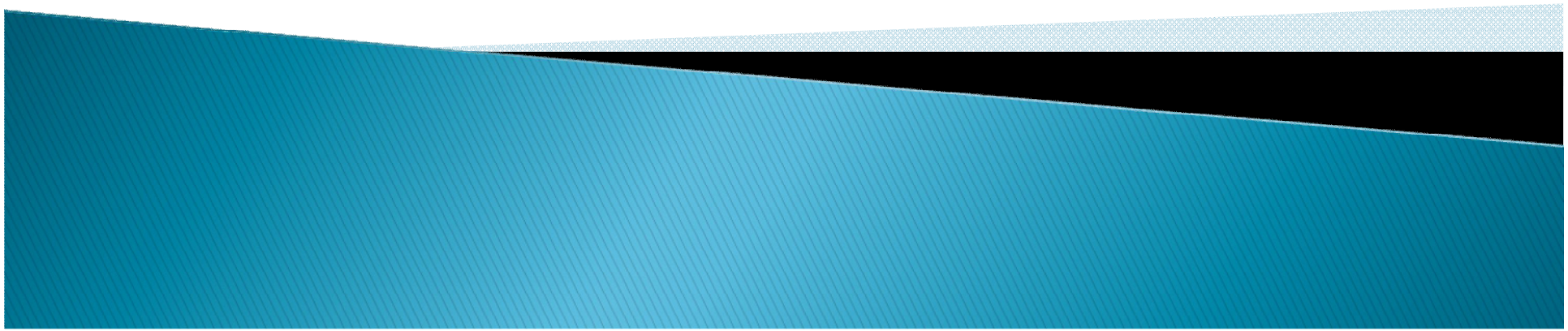
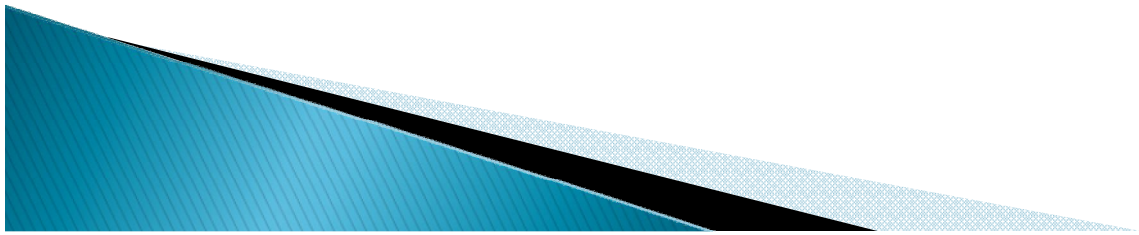
Szoftverfejlesztői követelmények minősített környezetben

Krasznay Csaba
Zrínyi Miklós Nemzetvédelmi Egyetem



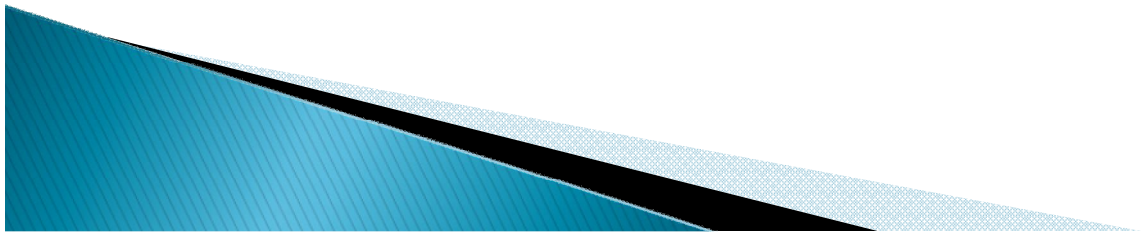
Bevezetés

- Korábban soha nem látott mennyiségű közigazgatási rendszer- és szoftverfejlesztés történik Magyarországon
- A Nemzeti Fejlesztési Ügynökség adatai szerint 38 nyertes projekt van csak az Elektronikus Közigazgatás Operatív Programon belül 49.105.493.163 Ft értékben
- Az új rendszerek a következő évtizedre meghatározzák a közigazgatási informatikát.
- A biztonságos tervezés, kivitelezés és üzemeltetés alapvető fontosságú!



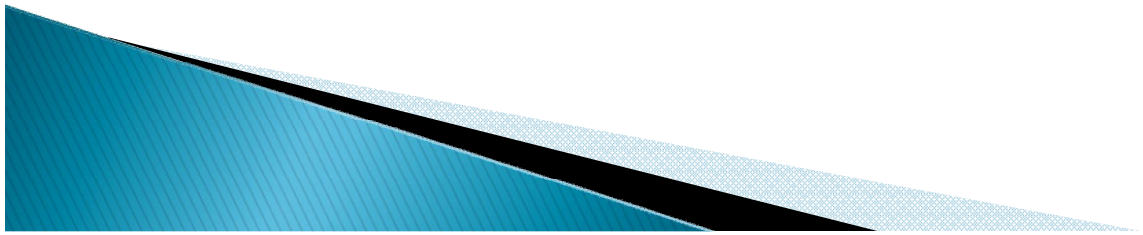
Fejlesztésbiztonsági követelmények

- Ahhoz, hogy a szükséges biztonsági szintet el lehessen érni a rendszerekben, a biztonságnak meg kell jelennie:
  - A tervezésben,
  - A dokumentálásában,
  - A fejlesztési folyamatokban,
  - A tesztelésben,
  - A sebezhetőség-vizsgálatban.
- Jelen előadás a fejlesztési folyamatokkal, azon belül is a fejlesztői környezet biztonságával foglalkozik.



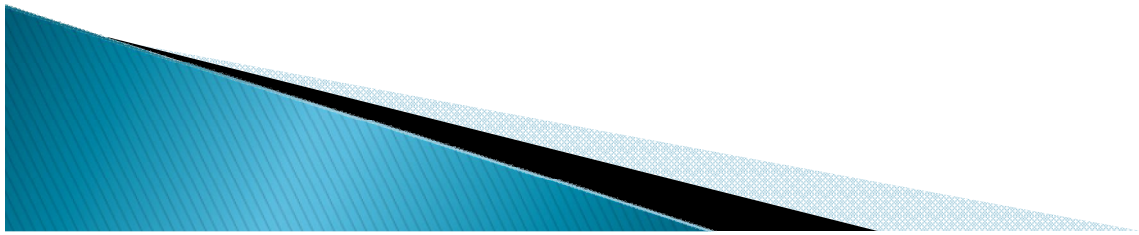
Jogszabályi háttér

- A minősített közigazgatási szoftverfejlesztésekre a következő jogszabályok vonatkozhatnak:
  - 1995. évi LXV. Törvény az államtitokról és a szolgálati titokról
  - 79/1995. (VI. 30.) Korm. Rendelet a minősített adat kezelésének rendjéről
  - 143/2004. (IV. 29.) Korm. rendelet az államtitkot vagy szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintő vagy különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól
- A fejlesztési folyamattal egyik jogszabály sem foglalkozik. Ma Magyarországon a jogszabályok nem foglalkoznak a területtel!



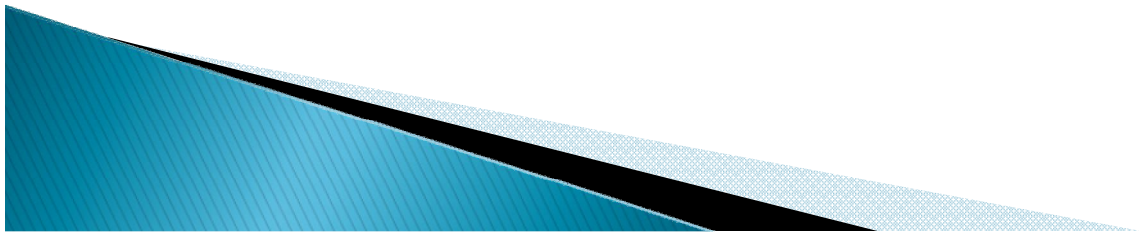
Ajánlások

- A Közigazgatási Informatikai Bizottság 25. és 28. számú ajánlásai már megemlítik, hogy a fejlesztői környezet biztonságával foglalkozni kell, de konkrét útmutatást nem tartalmaznak.
- Ma Magyarországon kis túlzással bárki, bárhol, bárhogy előállíthat minősített alkalmazást!!!
- A gyakorlatban természetesen ez nem így működik, de strukturált követelmények nincsenek.

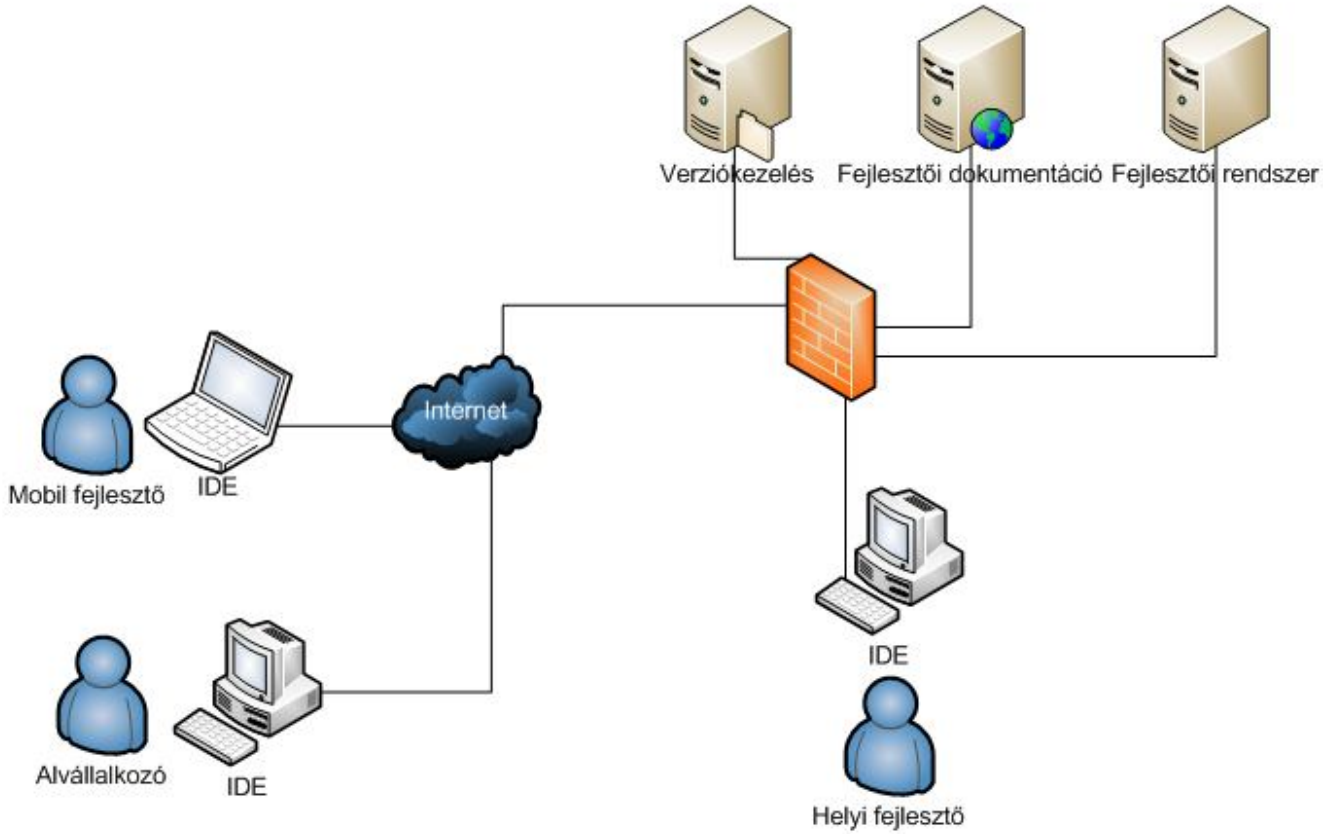


Javasolt lépések

- Meg kell határozni az elvárt biztonsági szinteket!
- Minden minősített fejlesztés esetén létre kell hozni a biztonságirányítás szervezetét!
- Fizikai, logikai és adminisztratív védelmi intézkedéseket kell kidolgozni a fejlesztői környezetre!



Tipikus fejlesztés



Biztonsági szintek

- A KIB 25. és 28. ajánlások szellemében három javasolt biztonsági szint:
  - államtitkot feldolgozó rendszerek (kiemelt biztonsági szint)
  - belső használatú, bizalmas információkat kezelő rendszerek (fokozott biztonsági szint)
  - széles körben, interneten keresztüli hozzáférést biztosító rendszerek (alap biztonsági szint)
- A KIB 28. ajánlással szemben nem komplex kockázatelemzés alapján dőlnek el a biztonsági szintek, hanem a hozzáférés alapján!

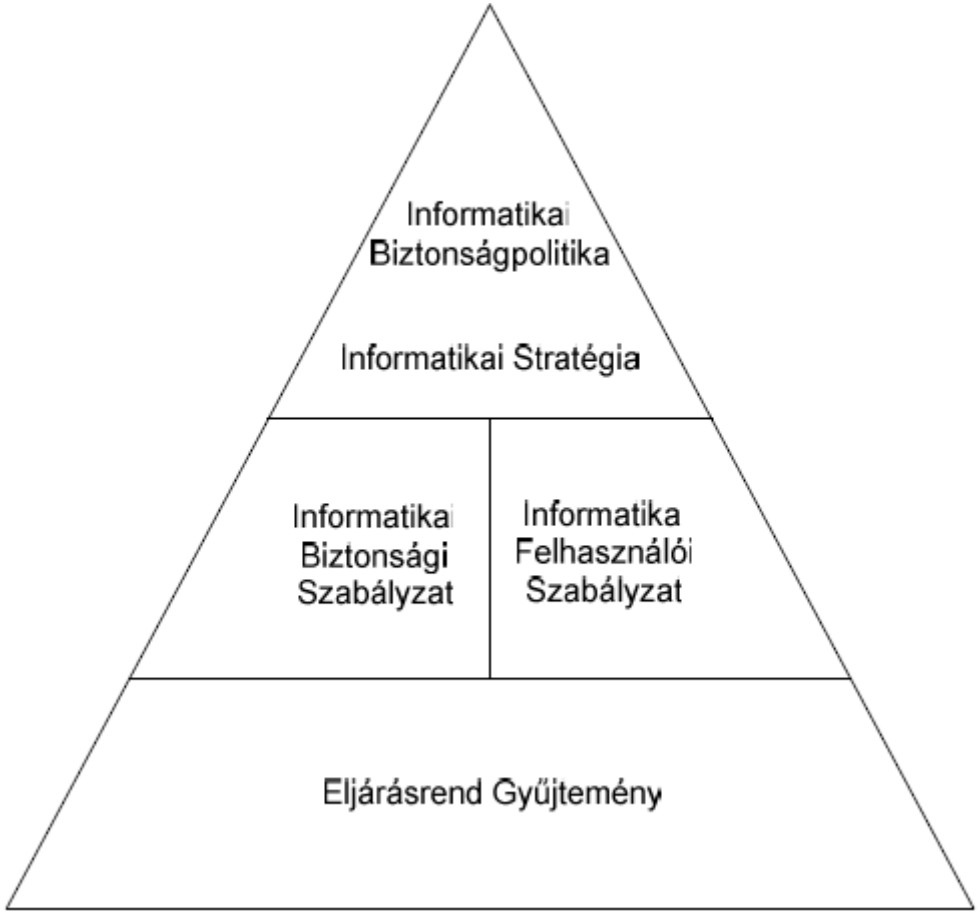
Személyi és szervezeti követelmények

- A KIB 25. ajánlás szerint minden érintett fejlesztésben létre kell hozni az Informatikai Biztonsági Fórumot, melynek tagjai:
  - A fejlesztő szervezet vagy a fejlesztési projekt vezetője,
  - Biztonsági Vezető,
  - Fejlesztési vezető,
  - Üzemeltetési Vezető.
- Munkájukat a projektiroda segíti
- Részletes feladataikat és felelősségüket ld. Hadmérnök 2010. 1. szám!

Személyi és szervezeti követelmények

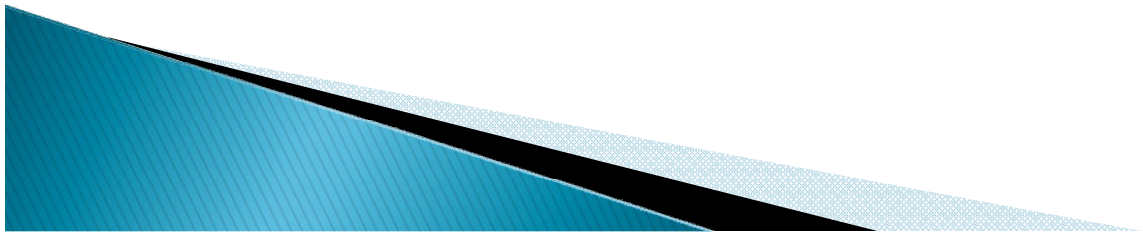
	Alap	Fokozott	Kiemelt
Projektvezető	A típusú ellenőrzés	B típusú ellenőrzés	C típusú ellenőrzés
Projektiroda munkatársai, a Biztonsági, Fejlesztési és Üzemeltetési Vezető	Erkölcsi bizonyítvány fokozott háttérellenőrzés sel, Biztonsági Vezetőnek CISM vizsga	A típusú ellenőrzés, Biztonsági Vezetőnek CISM vizsga	B típusú ellenőrzés, Biztonsági Vezetőnek CISM vizsga és TÜK bizonyítvány
Fejlesztők, üzemeltetők	Erkölcsi bizonyítvány	Erkölcsi bizonyítvány fokozott háttérellenőrzés sel	B típusú ellenőrzés

Szabályzati követelmények



Műszaki követelmények

- A KIB 28. alapján kerültek kidolgozásra.
- Az éles rendszerek követelményeit kellett átdolgozni a fejlesztési folyamatokra.
- Néhány helyen enyhíteni kellett/lehetett, hiszen
  - a fejlesztői környezetben még nem elsősorban üzleti adatokat kell védeni
  - a fejlesztői rendszerek pedig sokszor nem működnek megfelelően az éles környezet előírásaival
- Részletesen ld. Hadmérnök 2010. 2. szám!



Műszaki követelmények

	Biztonsági intézkedés neve	Alacsony	Fokozott	Kiemelt
		biztonsági osztály alapkonfigurációja		
Konfiguráció kezelés				
KK-1	Konfiguráció kezelési szabályzat és eljárásrend	KK-1	KK-1	KK-1
KK-2	Alap konfiguráció	KK-2	KK-2	KK-2
KK-3	Konfigurációváltozások	--	KK-3	KK-3
KK-4	A konfigurációváltozások felügyelete	--	KK-4	KK-4
KK-5	A változtatásokra vonatkozó hozzáférés korlátozások	--	KK-5	KK-5
KK-6	Konfigurációs beállítások	KK-6	KK-6	KK-6
KK-7	Legszűkebb funkcionalitás	--	KK-7	KK-7
KK-8	Informatikai rendszer komponens leltár	KK-8	KK-8	KK-8

Azonosítás és hitelesítés				
AH-1	Azonosítási és hitelesítési szabályzat és eljárásrend	AH-1	AH-1	AH-1
AH-2	Felhasználó azonosítása és hitelesítése	AH-2	AH-2	AH-2
AH-3	Eszközök azonosítása és hitelesítése	--	AH-3	AH-3
AH-4	Azonosító kezelés	AH-4	AH-4	AH-4
AH-5	A hitelesítésre szolgáló eszközök kezelése	AH-5	AH-5	AH-5
AH-6	A hitelesítésre szolgáló eszköz visszacsatolása	AH-6	AH-6	AH-6
AH-7	Hitelesítés kriptográfiai modul esetén	AH-7	AH-7	AH-7

Műszaki követelmények

Rendszer és információ sértetlenség				
RS-1	Rendszer és információ sértetlenségre vonatkozó szabályzat és eljárásrend	RS-1	RS-1	RS-1
RS-2	Hibajavítás	RS-2	RS-2	RS-2
RS-3	Rosszindulatú kódok elleni védelem	RS-3	RS-3	RS-3
RS-4	Behatolás észlelési eszközök és technikák	--	RS-4	RS-4
RS-5	Biztonsági riasztások és tájékoztatások	RS-5	RS-5	RS-5
RS-6	A biztonsági funkcionalitás ellenőrzése	--	--	RS-6
RS-7	Szoftver és információ sértetlenség	--	--	RS-7
RS-8	Kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelem	--	RS-8	RS-8
RS-9	A bemeneti információra vonatkozó korlátozások	--	RS-9	RS-9
RS-10	A bemeneti információ pontossága, teljessége és érvényessége	--	--	--
RS-11	Hibakezelés	--	--	--
RS-12	A kimeneti információ kezelése és megőrzése	--	--	--

Műszaki követelmények

Hozzáférés ellenőrzése				
HE-1	Hozzáférés ellenőrzési szabályzat és eljárásrend	HE-1	HE-1	HE-1
HE-2	Felhasználói fiókok kezelése	HE-2	HE-2	HE-2
HE-3	Hozzáférés ellenőrzés érvényre juttatása	HE-3	HE-3	HE-3
HE-4	Információ áramlás ellenőrzés érvényre juttatása	--	HE-4	HE-4
HE-5	A felelősségek szétválasztása	HE-5	HE-5	HE-5
HE-6	Legkisebb jogosultság	--	HE-6	HE-6
HE-7	Sikertelen bejelentkezési kísérletek	HE-7	HE-7	HE-7
HE-8	A rendszerhasználat jelzése	HE-8	HE-8	HE-8
HE-9	Értesítés előző bejelentkezésről	--	--	--
HE-10	Egyidejű munkaszakasz kezelés	--	--	--
HE-11	A munkaszakasz zárolása	--	HE-11	HE-11
HE-12	A munkaszakasz lezárása	HE-12	--	--
HE-13	Felügyelet és felülvizsgálat — hozzáférés ellenőrzés	HE-13	HE-13	HE-13
HE-14	Azonosítás és hitelesítés nélkül engedélyezett tevékenységek	HE-14	HE-14	HE-14
HE-15	Automatikus jelölés	--	--	--
HE-16	Automatikus címkézés	--	--	--
HE-17	Távoli hozzáférés ellenőrzése	HE-17	--	--
HE-18	A vezeték nélküli hozzáférésre vonatkozó korlátozások	HE-18	HE-18	--
HE-19	A hordozható és mobil eszközök hozzáférés ellenőrzése	HE-19	--	--
HE-20	Külső informatikai rendszerek használata	HE-20	HE-20	HE-20

Műszaki követelmények

Naplózás és elszámoltathatóság				
NA-1	Naplózási és elszámoltathatósági szabályzat és eljárásrend	NA-1	NA-1	NA-1
NA-2	Naplózandó események	NA-2	NA-2	NA-2
NA-3	A naplóbejegyzések tartalma	NA-3	NA-3	NA-3
NA-4	Napló tárkapacitás	NA-4	NA-4	NA-4
NA-5	Naplózási hiba kezelése	NA-5	NA-5	NA-5
NA-6	Napló figyelése, vizsgálata és jelentések készítése	--	NA-6	NA-6
NA-7	Naplócsökkentés, naplóriport készítés	--	NA-7	NA-7
NA-8	Időbélyegek	NA-8	NA-8	NA-8
NA-9	A napló információk védelme	NA-9	NA-9	NA-9
NA-10	Letagadhatatlanság	--	--	--
NA-11	A naplóbejegyzések megőrzése	NA-11	NA-11	NA-11

Műszaki követelmények

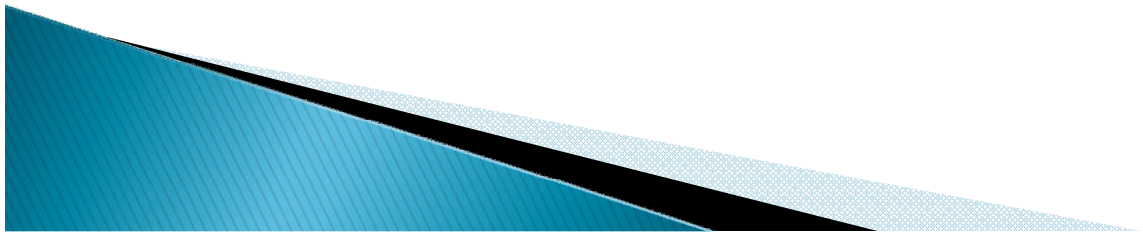
Rendszer és kommunikáció védelem				
RV-1	Rendszer és kommunikáció védelmi szabályzat és eljárásrend	RV-1	RV-1	RV-1
RV-2	Alkalmazás szétválasztás	--	RV-2	RV-2
RV-3	Biztonsági funkciók elkülönítése	--	--	RV-3
RV-4	Információ maradványok	--	--	--
RV-5	Szolgáltatás megtagadás elleni védelem	--	--	--
RV-6	Erőforrás prioritás	--	--	--
RV-7	A határok védelme	RV-7	RV-7	RV-7
RV-8	Az adatátvitel sértetlensége	RV-8	--	--
RV-9	Az adatátvitel bizalmassága	RV-9	--	--
RV-10	A hálózati kapcsolat megszakítása	--	--	--
RV-11	Megbízható útvonal	--	--	--
RV-12	Kriptográfiai kulcs előállítása és kezelése	RV-12	RV-12	RV-12
RV-13	Jóváhagyott kriptográfia alkalmazása	RV-13	RV-13	RV-13
RV-14	Sértetlenség védelem nyilvános hozzáférés esetén	--	--	--
RV-15	Telekommunikációs szolgáltatások korlátozása	RV-15	RV-15	RV-15
RV-16	Biztonsági paraméterek továbbítása	--	--	--
RV-17	Nyilvános kulcsú infrastruktúra tanúsítványok	--	RV-17	RV-17
RV-18	Mobil kód korlátozása	--	RV-18	RV-18
RV-19	Interneten Keresztüli Hangátvitel (VoIP)	--	RV-19	RV-19
RV-20	Biztonságos név/cím feloldó szolgáltatások (Hiteles forrás)	--	--	--
RV-21	Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)	--	--	--
RV-22	Architektúra és tartalékok név/cím feloldási szolgáltatás esetén	--	--	--
RV-23	Munkaszakasz hitelessége	--	--	--

Fizikai biztonsági követelmények

- Az informatikai rendszerek fizikai védelme jelenleg teljes mértékben mostohagyermeknek tekinthető.
- Sem a jogszabályok, sem az ajánlások nem adnak útmutatást arra, hogy milyen fizikai biztonsági intézkedéseket kell tenni.
- A 179/2003. (XI. 5.) Kormány rendelet II. fejezetével és ennek Nemzeti Biztonsági Felügyelet által kiadott dokumentumaival lehet analógiát vonni.
- Részletesen ld. Hadmérnök 2010. 2. szám!

Hogyan lehet ezt elérni?

- Common Criteria vagy KIB 25. szerinti fejlesztés: alap, közép és kiemelt szinten kötelező.
- ISO 27001 tanúsítvány a fejlesztési folyamatra: alap szinten opcionális, fokozott és kiemelt szinten kötelező.
- Nemzetbiztonsági ellenőrzés alatti fejlesztés: fokozott szinten opcionális, kiemelt szinten kötelező.



Összefoglalás

- A fejlesztői folyamatok biztonságát szabályozni kell, a lehető leghamarabb!
- Erre kitűnő lehetőséget nyújt a KIB 28. ajánlás.
- Mind a megrendelőnek, mind a fejlesztőnek, de leginkább Magyarországnak érdeke, hogy a közigazgatási rendszerek megfelelően és biztonságosan működjenek.
- Az erre irányuló ad hoc kezdeményezések helyett teljeskörű és összehasonlítható megoldásokra kell törekedni!

Köszönöm a figyelmet!

E-mail: csaba@krasznay.hu
Web: www.krasznay.hu