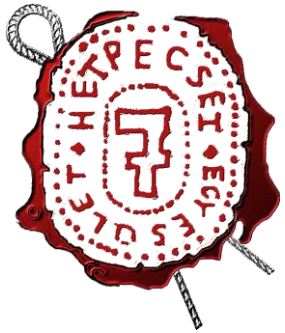
„Ha egy … diszciplína messzire távolodik tapasztalati forrásától, az súlyos veszélyt rejt magában. A forrásától eltávolodott folyó jelentéktelen ágak sokaságává különül el és a diszciplína részletek és bonyodalmak szervezetlen tömegévé válik.”

(Neumann János)

HUNGUARD

A 2013. évi L. törvény végrehajtási rendelete alapján folytatott biztonsági tanúsítások tapasztalatai a szolgáltatók széles körének vizsgálata után

dr. Szabó István
matematikus, egyetemi docens
szaboi@hunguard.hu
www.hunguard.hu



LXVIII. Szakmai fórum
2015. november 18.

A prezentáció felépítése:

- ***Jogszabályi környezet, a tanúsítások alanyai***
- ***Alkalmazott vizsgálati módszertan, követelmények***
- ***Tapasztalatok, összesített statisztikai adatok***
- ***Következtetések***

HUNGUARD

2007. évi LXXXVI. törvény a villamos energiáról /VET/
2008. évi XL. törvény a földgázellátásról /GET/
2011. évi CCIX. törvény a víziközmű-szolgáltatásról /VÍZ/
2003. évi C. törvény az elektronikus hírközlésről /EHT/

2007. évi LXXXVI. törvény 43. § :

*„(4) Számla kiállítására csak olyan informatikai rendszer felhasználásával kerülhet sor, amely … megakadályozza a számlázási rendszerhez történő jogosulatlan hozzáférést, valamint a számlázási információk észrevétlen módosítását. … Ennek érdekében a szolgáltatónak adminisztratív, fizikai és logikai intézkedésekkel biztosítania kell az **általános információbiztonsági zártsági követelmények** teljesülését.*

(5) A (4) bekezdésben meghatározott követelményeknek való megfelelést tanúsító szervezet által történő, a számlázási informatikai rendszerre vonatkozó tanúsítással kell igazolni. …

*(7) A … számlázási rendszer információbiztonsági megfeleltetéséről az engedélyes **az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény**nek megfelelően és módon köteles gondoskodni. …*

*(10)... A logikai védelmi intézkedések számlázó szoftverre vonatkozó követelményeinek vizsgálata során a nyilvános, nemzetközi sérülékenységi adatbázissal nem rendelkező **egyedi számlázó szoftverek esetén a vizsgálatnak ki kell terjednie a számlázó szoftver forráskódszintű elemzésére** is.”*

2013. évi L. törvény

77/2013. (XII.19.) NFM rendelet

az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

NIST SP 800 53 rev4
Security and Privacy Controls for Federal Information Systems and Organizations
2013 (464 pages)

National **I**nstitute of **S**tandards and **T**echnology **S**pecial **P**ublication

113 db. NIST SP 800 és 67 db. egyéb standard

NIST SP 800 53A rev4
Assessing Security and Privacy Controls in Federal Information Systems and Organizations
Building Effective Assessment Plans
2014 (399 pages)

Eljárások:
- Examination, Interview, Test

Vizsgálati jellemzők:
- Depth, Coverage
- Basic, Focused, Comprehensive

Ezek segítik az elvárások értelmezését, használatát.

Pl.: **NIST SP 800-30** Guide for Conducting Risk Assessments
NIST SP 800-55 Performance Measurement Guide for Information Security, …

77/2013 NFM 3.3.1. ≡ 41/2015 BM 3.3.6.

CSALÁD - KOMPONENS

3.3.1.	**Konfigurációkezelés**	
3.3.1.1.	Konfigurációkezelési eljárásrend	1
3.3.1.2.	Alapkonfiguráció	5
3.3.1.3.	A konfigurációváltozások felügyelete (változáskezelés)	3
3.3.1.4.	Biztonsági hatásvizsgálat	2
3.3.1.5.	A változtatásokra vonatkozó hozzáférés korlátozások	4
3.3.1.6.	Konfigurációs beállítások	3
3.3.1.7.	Legszűkebb funkcionalitás	4
3.3.1.8.	Elektronikus információs rendszerelem leltár	6
3.3.1.9.	Konfigurációkezelési terv	1
3.3.1.10.	A szoftverhasználat korlátozásai	1
3.3.1.11.	A felhasználó által telepített szoftverek	1
		31

Special Publication 800-53 Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

Configuration Management	
CM-1	Configuration Management Policy and Procedures
CM-2	Baseline Configuration
CM-3	Configuration Change Control
CM-4	Security Impact Analysis
CM-5	Access Restrictions for Change
CM-6	Configuration Settings
CM-7	Least Functionality
CM-8	Information System Component Inventory
CM-9	Configuration Management Plan
CM-10	Software Usage Restrictions
CM-11	User-Installed Software

Biztonsági szintek száma: **5** **3** (low, moderate, high)

Intézkedések (elvárások) száma a 77/2015 NFM r.-ben:

Biztonsági szint→	**1**	**2**	**3**	**4**	**5**	**Családok száma**
Adminisztratív int.	**13**	**23**	**49**	**61**	**67**	**7**
Fizikai intézkedések	**0**	**3**	**10**	**19**	**26**	**1**
Logikai intézkedések		**46**	**79**	**187**	**254**	**10**
Összesen:	**13**	**72**	**138**	**267**	**347**	**18**

2013. évi L. törvény

77/2013 NFM rendelet

41/2015 (VII. 15.) BM rendelet

NIST 800 53 rev4

6.§ (3):"… ha az elektronikus információs rendszer fejlesztése 2015.07.16-án a 77/2013. NFM rendelet előírásai szerint már folyik, az elektronikus információs rendszer e fejlesztésére a BM rendeletben foglaltakat 2015.10.01. napjától kell alkalmazni."

TABLE H-1: MAPPING NIST SP 800-53 TO ISO/IEC 27001

NIST SP 800-53 CONTROLS	ISO/IEC 27001 CONTROLS

TABLE H-2: MAPPING ISO/IEC 27001 TO NIST SP 800-53

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS

TABLE H-3: MAPPING ISO/IEC 15408 TO NIST SP 800-53

ISO/IEC 15408 REQUIREMENTS	NIST SP 800-53 CONTROLS

Tendencia: Konvergencia, pl. PP megfeleltetés pl.: https://www.niap-ccevs.org/pp/pp_app_v1.1-map.pdf

5

A 77/2013 NFM rendelet (NIST SP 800 53) elvárásain alapuló tanúsítási folyamat vázlata

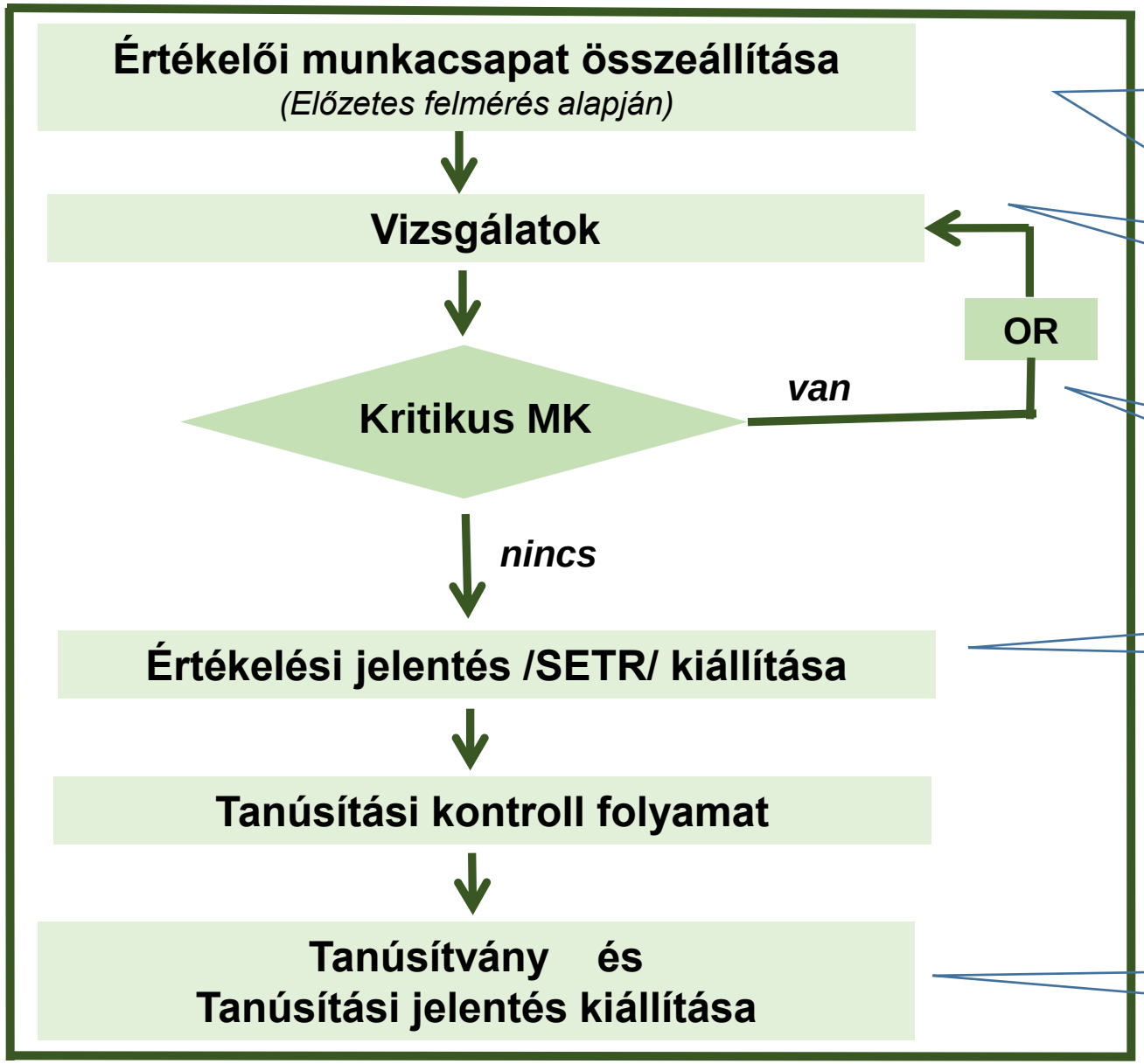
HUNGUARD

Értékelési folyamat

ISO 17025
General requirements for the competence of testing and calibration laboratories

Tanúsítási folyamat

ISO 17065
Requirements for bodies certifying products, processes and services



CISA: Certificated Information Systems Auditor
ISO 27001 auditor
CEH: Certified Ethical Hacking
ISTQB: Certified Tester Foundation Level
CISSP: Cert. Inf. Systems Security Professional
CISM: Certified Information Security Manager,...

Dokumentumok átvizsgálása, interjúk, rendszer-vizsgálatok, sérülékenység-tesztelés, forráskód-elemzés,…

OR: Observation Report (átlag 2-3)
MK: Maradvány kockázat

SETR: Security EvaulationTechnical Report

A nem kritikus MK-k jelzése a rendszer biztonsági szintjének elvárt növeléséhez

A 77/2013 NFM rendelet (NIST SP 800 53) elvárásain alapuló tanúsítások tapasztalatai

A tanúsított szervezetek száma 100-as nagyságrendű, melyekre a követelményeket a szervezet által jóváhagyott besorolás alapján többségében

Logikai biztonsági osztály **3.3.3.**
Adminisztratív biztonság osztály **1**
Fizikai biztonsági osztály **2** szinten vizsgáltuk.

Ez a besorolási szint a 77/2013 NFM r. szerint **95** követelmény vizsgálatát jelenti.

A vizsgálat fókusza:

- **van-e** az elektronikus információs rendszerben az elvárt követelményre alkalmazott intézkedés, eljárás;
- **milyen hatásfokú** az intézkedés.

Vizsgálatok eredményei

Van kritikus MK

Nincs kritikus MK → **A tanúsítvány kiállítható**

A **tapasztalatok** szerint pl. az alábbi vizsgálatok eredményezik:
a) Sérülékenység-tesztelés (penetration test, vulnerability scanning); → **BBT**: Black Box Test**, GBT:** Grey Box Test
b) Forráskód-elemzés;
c) Egyéb hiányosságok.

Általános tapasztalatok

Néhány cég kivételével, a vizsgált rendszerek informatikai biztonsági állapota nem volt kellően magas szintű.
A legkritikusabb problémák forrásai:

Az internetre kapcsolódó IT rendszerek 95%-ában a külső web-es sérülékenység vizsgálat során több kritikus, könnyen kihasználható sérülékenység is feltárásra került

41/2015 BM: 3.3.5.3. (77/2013 NFM 3.1.2.4.) **Sérülékenység teszt**
NIST 800-53: RA-5 VULNERABILITY SCANNING
„Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code review„

Tapasztalatok: A feltárt magas besorolású, könnyen ki-használható és magas hatásvektorú sérülékenységek 80%-át alacsony anyagi erőforrások ráfordításával javítani lehetett.

A forráskód-elemzés 85%-ban talált kritikus MK-t

41/2015 BM: 3.3.4.3. Speciális értékelés („…egyedi…forráskód elemzés…")
3.3.7.10. Bemeneti információ ellenőrzés

Törvényi előírás: „A logikai védelmi intézkedések számlázó szoftverre vonatkozó követelményeinek vizsgálata során a nyilvános, nemzetközi sérülékenységi adatbázissal nem rendelkező egyedi számlázó szoftverek esetén a vizsgálatnak ki kell terjednie a számlázó szoftver forráskódszintű elemzésére is"

Tapasztalatok: A legtöbb rendszerre (SAP, ORACLE) nem kellett elvégezni a „code-review" vizsgálatokat, de ahol el kellett végezni, ott 85%-ban súlyos hibák fordultak elő, pl.
- hiányos bemeneti információ ellenőrzés;
- jelszó-kezelés, napló-kezelés;
- SQL, LDAP fault injection sérülékenység;
- egyedi kriptográfiai algoritmusok, …

Ezek miatt a kezdeti értékelés a vizsgált rendszerek túlnyomó többségénél olyan **kritikus maradvány kockázatok**at tárt fel, melyek alapján
- mind a belső rendszerből (pl. egy rosszindulatú belső felhasználó által),
- mind kívülről (pl. egy hacker által)

a rendszer a siker esélyével támadható volt: lehetőség volt a rendszer teljesítményének, rendelkezésre állásának lerontására, vagy bizalmas adatokhoz való hozzáférésre, módosításra.

További tapasztalatok

HUNGUARD

Egyéb elvárások teljesítésének jelentős hiánya is a cégek többségénél jellemző volt:

- a szabályzatok, szükséges dokumentációk hiányosak voltak;
- sokszor elavult és sérülékeny szoftvereket használtak (pl. XP) ;
- a rendszerek jogosultsági és naplózási beállításai többségében a minimális elvárásoknak sem feleltek meg,
- az információbiztonsági felelősségi rendszer kialakításának a hiánya,……

Jelentős számban találtunk olyan védelmi intézkedéseket, melyek formálisan teljesítették a jogszabályi előírást, viszont – felhasználva a NIST 800 szabvány-család részletes szakmai ismertetőit – nem kellően erős, átfogó védelmi megoldásokat alkalmaztak.

Például kiemelünk ezekből kettőt:

3.3.4. Adathordozók védelme

3.3.4.1. Adathordozók védelmére vonatkozó eljárásrend
3.3.4.2. Hozzáférés az adathordozókhoz
3.3.4.3. Adathordozók címkézése
3.3.4.4.Adathordozók tárolása
3.3.4.5. Adathordozók szállítása
3.3.4.5.2. Kriptográfiai védelem
3.3.4.6. Adathordozók törlése
3.3.4.6.2. Ellenőrzés
3.3.4.6.3. Tesztelés
3.3.4.6.4. Törlés megsemmisítés nélkül
3.3.4.7. Adathordozók használata
3.3.4.7.2. Ismeretlen tulajdonos

3.3.5. Azonosítás és hitelesítés

3.3.5.1. Azonosítási és hitelesítési eljárásrend
3.3.5.2. Azonosítás és hitelesítés /8 komponens/
3.3.5.3. Eszközök azonosítása és hitelesítése
3.3.5.4. Azonosító kezelés
3.3.5.5. A hitelesítésre szolgáló eszközök kezelése
3.3.5.5.2. Jelszó (tudás) alapú hitelesítés
3.3.5.5.3. Birtoklás alapú hitelesítés
3.3.5.5.4. Tulajdonság alapú hitelesítés
3.3.5.5.5. Személyes vagy megbízható harmadik fél általi regisztráció
3.3.5.6. A hitelesítésre szolgáló eszköz visszacsatolása
3.3.5.7. Hitelesítés kriptográfiai modul esetén
3.3.5.8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

3.3.4.6. Adathordozók törlése (41/2015. BM: 3.3.8.6.)

HUNGUARD

3.3.4.6.1. Az érintett szervezet:

3.3.8.4.1.1. a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törli az elektronikus információs rendszer meghatározott adathordozóit a leselejtezés, a szervezeti ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás előtt;

3.3.8.4.1.2. a törlési mechanizmusokat az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően alkalmazza.

NIST Special Publication 800-88
Revision 1

Guidelines for Media Sanitization

Paper and microforms

Mobil phones, smart phones, PDAs, tablets, …

Copy, print, fax, and multifunction machines

CD, DVD, BD

USB

!!!

3.3.5.5.2. Jelszó (tudás) alapú hitelesítés (41/2015 BM: 3..3.9.5.2.)

HUNGUARD

Leggyakrabban **meghatározzák a jelszó-policy-t**: ez szükséges, de az elektronikus információs rendszer ritkán kényszeríti ki a jelszó-policy betartását.
(77/2013 NFM 3.3.5.5.2.1.1.: „a jelszóra … elvárásokat érvényesíti…)

NIST SP 800-53, Appendix F-IA, IA-5

AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

The information system, for password-based authentication:

(a) Enforces **minimum password complexity** of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];*

(b) Enforces at least the following number of changed characters when new passwords are created: [*Assignment: organization-defined number];*

(c) **Stores and transmits only cryptographically-protected passwords**;

(d) Enforces **password minimum and maximum lifetime restrictions** of [*Assignment: organization-defined numbers for lifetime minimum, lifetime maximum];*

Leggyakrabban van előírás a maximális élettartamra, de nincs előírás a minimális élettartamra

Több esetben nem volt védelem, a jelszavakat nyíltan (clear text vagy base64) tárolták, viszont ahol használtak kriptográfiai védelmet, ott is túlnyomó többségnél gond van a védelem megfelelőségével

3.3.5. Azonosítás és hitelesítés
3.3.5.5. A hitelesítésre szolgáló eszközök kezelése
3.3.5.5.2. Jelszó (tudás) alapú hitelesítés

HUNGUARD

NIST Special Publication 800-63-2

Electronic Authentication Guideline

Table A.1 – Estimated Password Guessing Entropy in bits vs. Password Length

	User Chosen			Randomly Chosen		
	94 Character Alphabet			10 char. alphabet		94 char alphabet
Length Char.	No Checks	Dictionary Rule	Dict. & Composition Rule			
1	4	-	-	3	3.3	6.6
2	6	-	-	5	6.7	13.2
3	8	-	-	7	10.0	19.8
4	10	14	16	9	13.3	26.3
5	12	17	20	10	16.7	32.9
6	14	20	23	11	20.0	39.5
7	16	22	27	12	23.3	46.1
8	18	24	30	13	26.6	52.7
10	21	26	32	15	33.3	65.9
12	24	28	34	17	40.0	79.0
14	27	30	36	19	46.6	92.2
16	30	32	38	21	53.3	105.4
18	33	34	40	23	59.9	118.5
20	36	36	42	25	66.6	131.7
22	38	38	44	27	73.3	144.7
24	40	40	46	29	79.9	158.0
30	46	46	52	35	99.9	197.2
40	56	56	62	45	133.2	263.4

A vizsgálatok tapasztalatai:

széles körben nem megfelelő a hitelesítés-kezelés a „brute force attack” ellen:

a) több rendszerben nincs korlátozva a belépési próbálkozások száma, vagy idő-intervalluma;

b) a letárolt jelszókép kipróbálása ellen

= nem kellően erős a használt hash függvény;

= nem szerepel (a NIST SP 800-53, Append. F-IA-5-ben említett) „sózás”;

= nem alkalmazzák a hash-t nagy számú ciklusban (pl. a PBKDF2, Bcrypt, Scrypt szabványok szerint)

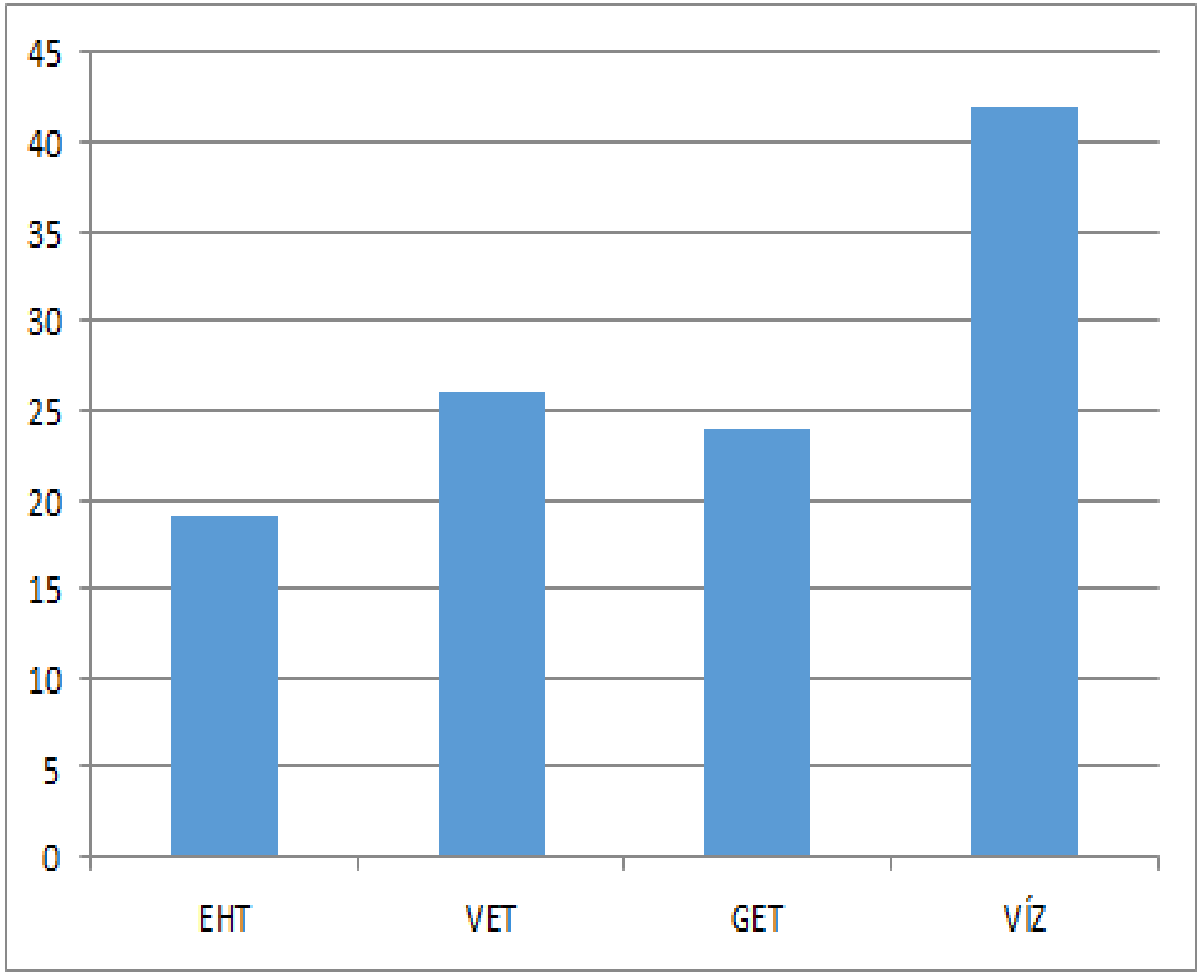
Az eddig említett (és más) hiányosságok

- egy része kritikus MK, melyeket a tanúsítási folyamat folytatása előtt javítani kellett,
- másik része „enyhébb nem megfelelőség”-nek minősíthető, melyek nem jelentenek közvetlen kockázatot a rendszer biztonságára, de hosszabb távon javítandók. Ezeket a kockázataik alapján 3 kategóriába sorolva (1,2,3 szintű MK /az 1 a legalacsonyabb/) tartalmazza a Tanúsítási jelentés.

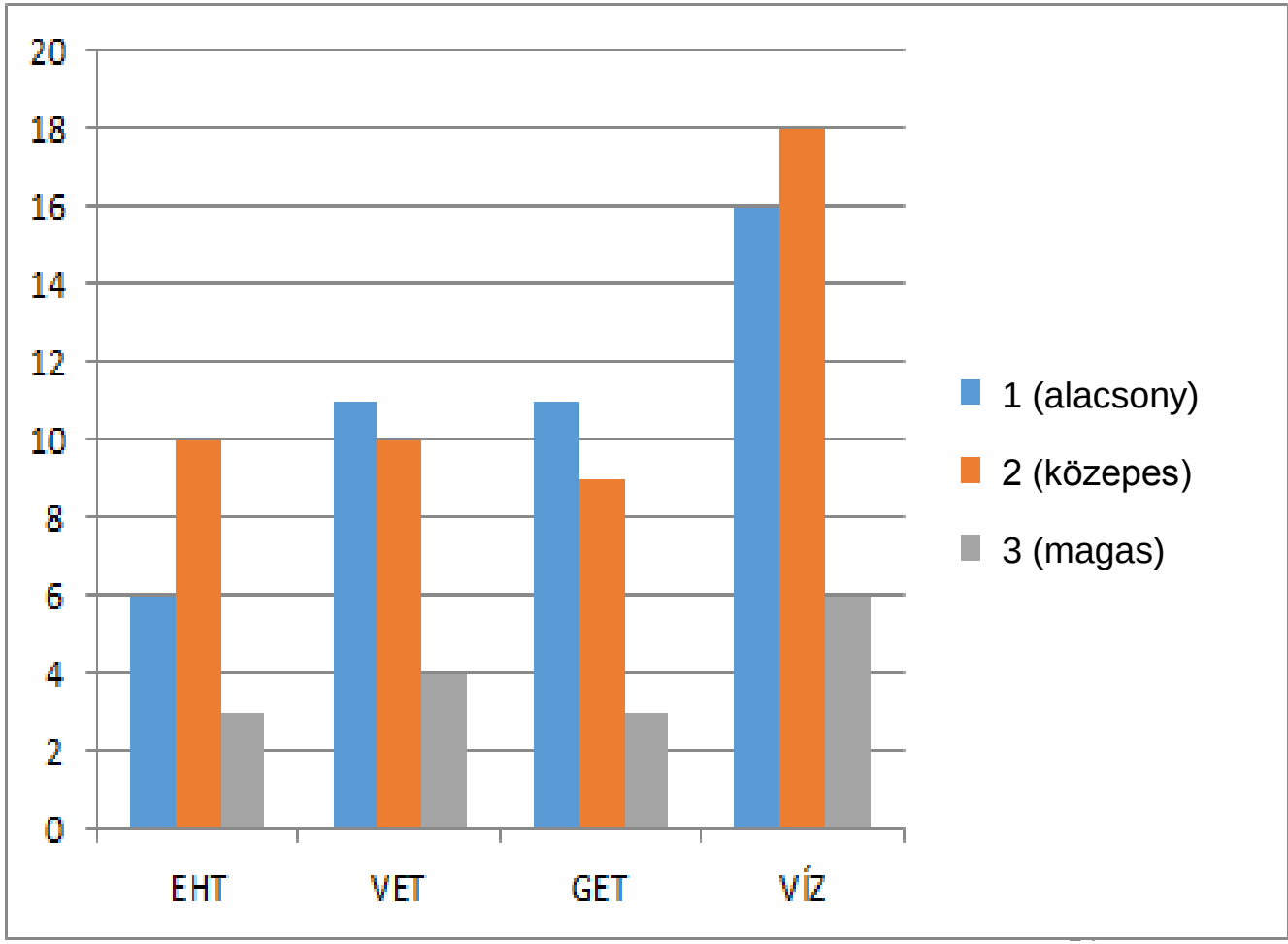
A tanúsítási folyamat végén (0 db. kritikus MK mellett) **az „enyhe nem-megfelelőségek” aránya:**

Intézkedés- csomag	A nem kritikus problémák száma %-ban
Adminisztratív védelem	**15,4**
Fizikai és környezeti védelem	**2,8**
Logikai védelem	**81,8:**
Konfigurációkezelés	**13,1**
Üzletmenet (ügymenet) folytonosság tervezése	**9,1**
Karbantartás	**3,1**
Adathordozók védelme	**6,1**
Azonosítás és hitelesítés	**12,5**
Hozzáférés ellenőrzése	**7,3**
Rendszer- és információsértetlenség	**8,7**
Naplózás és elszámoltathatóság	**10,3**
Rendszer- és kommunikációvédelem	**5,3**
Reagálás a biztonsági eseményekre	**6,3**

A maradványkockázatok átlagos száma szektoronként a tanúsítási folyamat végén:



A maradványkockázatok súlyosság szerinti megoszlása szektoronként a tanúsítási folyamat végén:



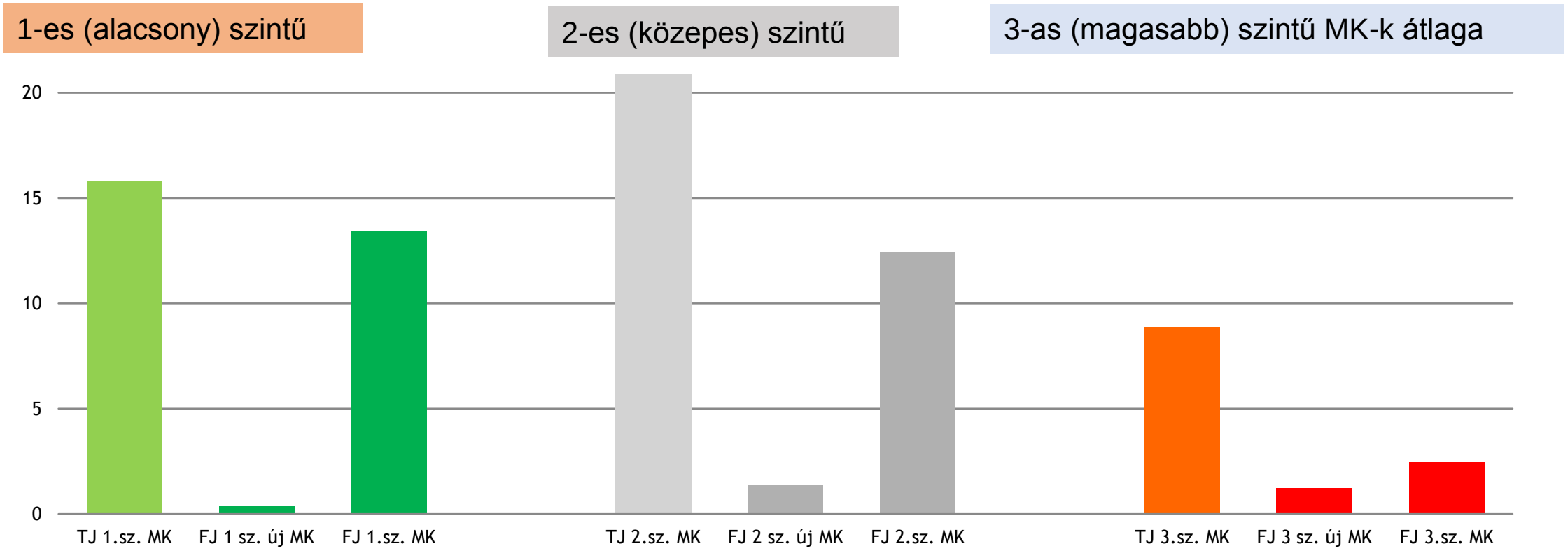
FELÜLVIZSGÁLATI EREDMÉNYEK

A kezdeti tanúsítás után a vizsgált rendszerekben (IT, működtetés, szabályozás) jelentős változások történtek:

- részben a működtetés igényei alapján;
- részben a Tanúsítási jelentésben szereplő MK-k csökkentése miatt.

A felülvizsgálatok során a sérülékenység-tesztelés újabb, **átlag 4,88** számú, javítandó hibát jelzett.

A maradványkockázatok átlagos számának változása az első felülvizsgálatban résztvevő szervezeteknél:



TJ: Tanúsítási jelentésben jelzett **MK-k átlaga** (ahol már volt felülvizsgálat)
FJ új: Felülvizsgálat során a rendszer továbbfejlesztése alapján bekerült **új MK-k**
FJ: A felülvizsgálat **összesített MK-k átlaga** (megmaradt és új MK-k)

KÖVETKEZTETÉSEK

HUNGUARD

1. Az első értékelési folyamatban már javításra kerültek a kritikus hibák.
2. A kezdeti értékelési és tanúsítási folyamat eredményei alapján a kritikus kockázatok kiküszöbölése után is jelentős számú kockázati tényező maradt, melyek javításával a rendszerek biztonsági szintje tovább növelhető.
3. A meghatározott idő utáni (ennek megfelelően továbbfejlesztett rendszerekre vonatkozó) felülvizsgálati rendszerértékelés eredményei:
   - új kritikus (javítandó, döntően internetes támadást lehetővé tévő újonnan bekerült) kockázatok keletkeztek;
   - a felülvizsgálati eljárásban a kockázati mérték átlag **46,6 %**-os csökkenést eredményezett (16-70 % közötti értékekkel) a súlyozott mérőszámmal mért maradvány kockázatok (nem-megfelelőségek) értékében a kezdeti értékeléshez képest .

A fentiek alapján
- Egyrészt **lényegesen javult a szektorban az informatikai biztonság általános szintje**;
- Magasabb szintre emelkedett a szektorra vonatkozó **jogszabályi elvárásoknak megfelelés.**

Megjegyzés: **Más jogszabályok** is kötelezettségeket rónak (megsértés esetén büntető szankciókkal fenyegetve) az üzemeltetőre, munkatársaikra, melyeknek **megfelelést is segítette a tanúsítás**, pl. a személyes adatok védelmét előíró 2011. évi CXII. Törvény:

7. § (2) Az adatkezelő … köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek …az …adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

(3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, … ellen.

(6) Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

KÖSZÖNÖM A FIGYELMET!