Információbiztonság: az ISO 27001 információbiztonsági irányítási rendszer 2. rész

Előző számunkban közölt cikkben igyekeztünk felhívni a figyelmet, hogy egyre nagyobb szükség van arra, hogy a biztonság egyes szakterületein tevékenykedő szakemberek átlássák a „teljes képet". Annál is inkább így van ez, hiszen a támadónak elegendő egy rést találni a teljes rendszerben ahhoz, hogy bejusson, ezért a vállalatbiztonság területén kiemelt és egyre növekvő szerep jut az információbiztonságnak. Tanulmányunkban a biztonságtechnikát igyekszünk közelíteni az információbiztonsághoz. Amennyiben egy cégnél nem megalapozott az információbiztonság, akkor a biztonság egyéb követelményei sem tudnak maradéktalanul teljesülni. Ehhez nélkülözhetetlen a szabványkörnyezet alapos tanulmányozása.

Első cikkünkben az információbiztonsági irányítási rendszerek kiépítését elősegítve az ISO/IEC 27001:2005 szabványra hívtuk fel a figyelmet amely egy információbiztonsági irányítási rendszer kialakítását és ellenőrzését támogatja. Majd ehhez kapcsolódva ismertettük a fontos és hasznos útmutatásokat adó ISO 27000 szabványcsaládot.

■ Jelen dolgozatban az ***MSZ ISO/IEC 27001:2006 szabvánnyal*** foglalkozunk a továbbiakban, azonban fontos látni, hogy a teljes szabványcsalád hogyan épül fel, illetve melyek a fejlődés útjai. *(Amennyiben az első cikket esetleg nem olvasták, a téma teljes áttekintését nyilván segíti, ha a már megjelent cikkünket is hozzáférhetővé teszszük. lásd: detektor online / szakcikkek / szabályozás menüpont – a szerk.)*

AZ ISO 27001 RENDSZERE [1] [4-11]

Az információ bármely üzleti tevékenység alapja. A vállalkozás működése kerülhet veszélybe, ha az információk előállítása, tárolása, hozzáférésének szabályozása és kezelése nem biztonságos. Egy szabványos IBIR (Információ Biztonsági Irányítási Rendszer) – mint amilyen az ISO 27001 is – létrehozása, működtetése segít a vállalatnak abban, hogy az információbiztonsággal kapcsolatos, számára releváns kockázatokat feltárja, megismerje, kezelje. Ma már elmondható, hogy egy ilyen rendszer hiánya versenyhátrányt jelent.

Egy információbiztonsági irányítási rendszer kialakítása mindig kockázatelemzéssel kezdődik.

A kockázatok felmérése után a szabvány 11 védelmi területet jelöl meg:

- Biztonsági szabályzat,
- Az információbiztonság szervezete,
- Vagyontárgyak kezelése,
- Az emberi erőforrások biztonsága,
- Fizikai védelem és a környezet védelme,
- A kommunikáció és az üzemeltetés irányítása,
- Hozzáférés-ellenőrzés,
- Beszerzés, fejlesztés, fenntartás,
- Információbiztonsági incidensek kezelése,
- A működés folytonosságának irányítása,
- Jogi és műszaki megfelelőség.

Egy információbiztonsági rendszer legalább az információk alábbi tulajdonságait kell, hogy biztosítsa, az üzleti érdekek szerint elfogadható kockázatok mellett [6]:

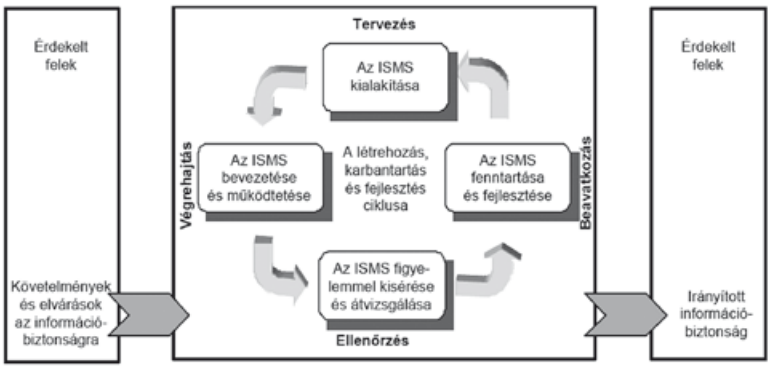
■ ***Bizalmasság*** *(Confidentiality):* Olyan tulajdonság, amely biztosítja, hogy az információt jogosulatlan egyének, entitások vagy folyamatok számára nem teszik hozzáférhetővé, és nem hozzák azok tudomására, azaz az értékes és érzékeny információkat óvja meg a jogosulatlan hozzáféréstől és kiszivárgástól. Az információhoz az, és csakis az férhet hozzá, akinek feladata van vele kapcsolatban.

■ ***Sértetlenség*** *(Integrity):* A vagyontárgyak pontosságának és teljességének védelmét biztosító tulajdonság, amely célja, hogy az információkezelés, -feldolgozás közben véletlenül ne sérülhessenek ezek a szempontok.

■ ***Rendelkezésre állás*** *(Availibility):* Olyan tulajdonság, amely lehetővé teszi, hogy az adott objektum – feljogosított entitás által támasztott igény alapján – hozzáférhető és igénybe vehető legyen. Másképpen fogalmazva, az információk és szolgáltatások minden, az adott ügyben illetékes alkalmazottnak tervezett és dokumentált módon rendelkezésére állnak.

Az ellenőrzés céljait érdemes közvetlenül az adott intézmény stratégiai céljaihoz kötni, hiszen mind az információbiztonság-

1. ábra: Az IBIR (ISMS) folyamata



forrás: www.crysys.hu/courses/adatbiztonsag/szabvanyok.pdf

nak, mind az erre vonatkozó ellenőrzésnek közvetlenül ezeket kell szolgálnia. [4]
Ezeket a kritériumokat ki lehet a vállalati működésre is terjeszteni. [12]

■ Az ISO 27001 nem technikai szabvány, hanem folyamatszemlélet-megközelítésű, a kockázatok felmérése és értékelése által vezérelve. Mint a legtöbb ISO/IEC szabvány, ez is a Plan-Do-Check-Act, röviden PDCA modellt használja, aminek magyar jelentése Tervezés, Végrehajtás, Ellenőrzés, Beavatkozás. ***(1. ábra)***

- ***Tervezés:*** célok, folyamatok és eljárások meghatározása illetve kialakítása, amelyek a kockázatok kezelése és az információbiztonsági rendszer fejlesztése során a vállalat általános üzleti politikáját szolgálja.
- ***Végrehajtás:*** információbiztonsági politika, intézkedések, folyamatok és eljárások bevezetése és működtetése.
- ***Ellenőrzés:*** a működés teljesítményének mérése és értékelése.
- ***Beavatkozás:*** az ellenőrzési folyamat alapján kapott eredmények alapján az információbiztonsági rendszer folyamatos fejlesztése.

AZ ISO 27001 A BIZTONSÁGTECHNIKAI MÉRNÖKI SZAKMÁBAN

A biztonságtechnikai mérnököknek elengedhetetlenül fontos a vonatkozó szabványok ismerete. Az alapvető biztonságtechnikához kapcsolódó szabványokon túlmenően azonban egyre fontosabb az irányítási szabványok ismerete. A teljesség igénye nélkül álljon itt néhány szempont:

- A kockázatértékelési és -csökkentési módszerek és eljárások kiválóan használhatók a vagyonvédelmi és biztonsági feladatoknál egyaránt.
- A dokumentációs és adminisztratív előírások alapot adnak a fizikai védelmi rendszerek működtetéséhez.
- Fontos, hogy egy biztonsággal foglalkozó mérnök értse az üzleti megközelítést.
- Nyelvezetet és eszközrendszert ad ahhoz, hogy a felsővezetéssel vagy menedzsmenttel érdemben tudjon tárgyalni.
- Folyamatszemléletet ad, amely szintén jól használható a mindennapi munkában.
- Vállalkozóként keretrendszert ad a komoly cégekkel történő együttműködésben.
- Vagyonvédelemmel foglalkozó cégeknél akár a szabvány egyes részeinek bevezetése is egy kész, formalizált működést eredményezhet, ami komoly versenyelőnyt jelenthet a szolgáltatási szint növekedése, vevői elégedettség, hatékonyabb működés és teljesítményhez kötött javadalmazáson keresztül.
- Egyre több vállalat/szervezet tanúsíttatja magát az ISO 27001 szerint, ezután persze így is kell működniük, hiszen a tanúsítvány megtartásának feltétele a rendszeres felülvizsgálatokon való megfelelés.
- Másrészt egyre szélesebb körben terjed az ISACA (Information Systems Audit and Control Association) módszertana és egyéb anyagai, több helyen már meg is követelik a CISA[1], CISM5[2], CRISC[3] vagy CGEIT[4] minősítést.
- Az (ISC)[2] (International Information Systems Security Certification Consortium) által jegyzett CISSP[5] minősítés is jó ajánlólevél a szakmában.
- A nemzetközi, de a hazai szakmai életben is egyre nagyobb szerepe van a szabványok ismeretének, és az ezekhez kapcsolódó szakmai szervezetek által kidolgozott minősítéseknek.
- A szabvány ismerete egy olyan eszközt ad a mérnök kezébe, amivel átfogóan tudja értékelni az adott feladatot, projektet, szervezetet.

Otti Csaba *(Óbudai Egyetem, Bánki Donát Kar, Alkalmazott Biometria Intézet, mérnök-közgazdász) –* ***magánbiztonsági szakértő*** *– otti.csaba@bgk.uni-obuda.hu*

Rónaszéki Péter *(ISACA Magyarország Egyesület, elnökségi tag) CISA, CISM, ISO27001LA –* ***információbiztonsági szakértő*** *– peter.ronaszeki@isaca.hu*

[1] *CISA – Certified Information Systems Auditor. Az ISACA által kidolgozott minősítés.*
[2] *CISM – Certified Information Security Manager. Az ISACA által kidolgozott minősítés.*
[3] *CRISC – Certified in Risk and Information Systems Control – Az ISACA által kidolgozott minősítés*
[4] *CGEIT – Certified in Governance Enterprise IT. Az ISACA által kidolgozott minősítés.*
[5] *CISSP – Certified Information Systems Security Professional – Az ISC(2) által kidolgozott minősítés.*

IRODALOMJEGYZÉK

[1] *MSZ ISO/IEC 27001:2006*
[2] *ISO/IEC 27001:2005*
[3] *ISO 27001 Series Update. 2012. január*
[4] *Szenes, K.: Serving Strategy by Corporate Governance – Case Study: Outsourcing of Operational Activities Procds. of 17th International Business Information Management Association – IBIMA November 14-15, 2011, Milan, Italy, ed. Khalid S. Soliman, ISBN: 978-0-9821489-6-9 © 2011 IBIMA, [CD-ROM], 2387–2398*
[5] *Enterprise Governance Against Hacking. Procds. of the 3rd IEEE International Symposium on Logistics and Industrial Informatics – LINDI 2011 August 25–27, 2011, Budapest, Hungary, ISBN: 978-1-4577-1840 © 2011 IEEE, IEEE Catalog Number: CFP1185C-CDR [CD-ROM], 229–233*
[6] *Szenes, K.: Supporting Applications Development and Operation Using IT Security and Audit Measures in: e-Informatica Software Engineering Journal, Volume 6, Issue 1, 2012, pages: 27–37, DOI 10.5277/e-Inf120102*
[7] *Vasvári György: Vállalati biztonságirányítás (Informatikai biztonságmenedzsment). Time-Clock Kft., 2007*
[8] *Muha Lajos (szerk.): Az informatikai biztonság kézikönyve. Verlag-Dashöfer, Budapest, 2000.*
[9] *Muha Lajos–Bodlaki Ákos: Az informatikai biztonság. Pro-Sec Kft., Budapest, 2003.*
[10] *Ködmön István (szerk.): Hétpecsétes történetek (Információbiztonság az ISO 27001 tükrében). Hétpecsét Információbiztonsági Egyesület, Budapest, 2008.*
[11] *Krasznay Csaba: Szabványok, ajánlások, modellek; http://www.crysys.hu/courses/adatbiztonsag/szabvanyok.pdf*
[12] *Szenes Katalin: Informatikai biztonsági módszerek kiterjesztése a vállalatirányítás, a működés, és a kockázatkezelés támogatására. Minőség és Megbízhatóság; nemzeti minőségpolitikai szakfolyóirat kiadja: az European Organization for Quality (EOQ) Magyar Nemzeti Bizottsága B/SZI/1993. HU ISSN0580-4485 XLVI. évf. 2012. / 5. sz., 252–257. old.*