Információbiztonság: az ISO 27001 információbiztonsági irányítási rendszer 1. rész

Összenő ami összetartozik. Az elmúlt 20 évben a biztonsággal foglalkozó szervezetek, elméletek markánsan elkülönültek egymástól. Azonban a globalizálódással és az intelligens bűnözés fejlődésével a rosszindulatú támadóknak egyre nagyobb eszköztár áll rendelkezésére a cselekmény elkövetésére.
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.
Jelen tanulmányunkban a biztonságtechnikát igyekszünk közelíteni az információbiztonsághoz.

De miről is beszélünk pontosan? ***15 évvel ezelőtt egy vállalat működési biztonsági kérdéseinél még fel sem merült az információbiztonság, mint fókusz.*** Hiszen ha meg tudtuk védeni értékeinket fizikailag a támadóktól, akkor az információink is biztonságban voltak. Ez történt élőerővel, mechanikai és elektronikai védelmi rendszerekkel. Napjainkban az információ egyre nagyobb érték és naponta több száz véletlenszerű vagy célzott támadás érkezik az internet irányából. 7 évvel ezelőtt ahhoz, hogy egy vállalat befolyásos személyeiről olyan adatokat gyűjtsenek, amivel vissza lehet élni, titkosszolgálati módszerekre volt szükség. Ma ennek a feladatnak a 80 százaléka elvégezhető a facebookról. Ezért ***fontos az, hogy a klasszikus védelmi területeken túlmenően az információbiztonsági elvekkel is tisztába legyenek a biztonságtechnikai mérnökök.***

■ ***Az ISO/IEC 27001:2005 szabvány egy információbiztonsági irányítási rendszer kialakítását és ellenőrzését támogatja.*** Fontos és hasznos útmutatásokat ad a rendszer kialakításához és értékeléséhez is. Az ISO 27000 szabványcsalád többféle információbiztonsági kérdést is tárgyal, ha nem is az összeset, hiszen például a kockázatmenedzsmenttel az ISO 31010, az üzletmenet-folytonossággal foglalkozó szabvány pedig az ISO 22301-es számot kapta. Az információbiztonsági irányítási rendszerek egyre nagyobb hangsúlyt kapnak a vállalatok és szervezetek működésében, e szabvány szerint tanúsíttathatják is magukat. Alapvető fontosságú tehát, hogy e szabványokat egy biztonságtechnikai mérnök is behatóan ismerje, hiszen ha egy ilyen keretrendszer kerül alkalmazásra akkor minden biztonsági alrendszer ide kell, hogy betagozódjon.

BEVEZETÉS [1][2][3]

Az ISO/IEC 27000 szabványsorozat egy olyan információbiztonsági szabványcsalád, amit a Nemzetközi Szabványügyi Szervezet (International Organization for Standardization – ISO) és a Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Comission – IEC) közösen fogadott el és adott ki.

■ A 27000-es sorozat egy egységes keretrendszerben azokat az összegyűjtött ajánlásokat tartalmazza, amelyekben az információbiztonság irányítási, kockázatértékelési és ellenőrzési feladatai lettek összefoglalva. Ezt a keretrendszert nevezzük Információbiztonsági Irányítási Rendszernek, amelyet a magyarban IBIR-nek is rövidítenek (angolul: Information Security Management System – ISMS).

■ A szabványsorozat felépítése hasonló az ISO 9000-es minőségirányítási és az ISO 14000-es környezetvédelmi rendszerek kialakításához. Ezen rendszerek úgy kerültek megalkotásra, hogy ha egy szervezet bármelyiket alkalmazza, akkor egy újabb rendszer már a bevezetésekor képes legyen illeszkedni az előzőhöz. Napjainkban pedig egyre terjed az a gyakorlat, hogy egy szervezet integrált irányítási rendszerben gondolkodik, például egyszerre vezetnek be ISO 9001-et és ISO 27001-et is.

AZ ISO 27000 SZABVÁNYCSALÁD FELÉPÍTÉSE [3]

Érdemes végigvenni, hogy az ISO 27000 szabványcsalád milyen szabványokból épül fel és azok mely területeket szabályoznak.

A szabványcsaládot az ISO/IEC szervezetek a BS brit szabványok (BS7799) átvételével hozták létre, ezeket a Magyar Szabványügyi Testület honosítja Magyarországon. A szabványcsalád 2012 januárjában aktuális teljes rendszere (azon szabványok ahol nincs évszám, még nem kerültek elfogadásra):

- ISO 27000:2009 – Információ technológia, Biztonsági technikák, ISMS – áttekintés és magyarázatok
- ***ISO 27001:2005 = MSZ ISO/IEC 27001:2006 – Információbiztonsági Irányítási Rendszerek – követelmények: „Ez a nemzetközi szabvány abból a célból készült, hogy modellként szolgáljon információbiztonsági irányítási rendszerek (ISMS) kialakításához, megvalósításához, működtetéséhez, figyelemmel kíséréséhez, átvizsgálásához, fenntartásához és fejlesztéséhez."*** [1]
- ISO 27002:2005 – Gyakorlati kézikönyv az ISMS rendszerek kialakításához
- ISO 27003:2010 – Bevezetési útmutató
- ISO 27004:2009 – Szabvány az információbiztonság számszerűsítéséről és mérési lehetőségeiről
- ISO 27005:2011 – Információbiztonsággal kapcsolatos kockázatok kezelése
- ISO 27006:2011 – Tanúsító és auditáló

szervezetek számára előírt követelmények
- ISO 27007:2011– Útmutató ISMS rendszerek auditálásához
- ISO 27008:2011– Útmutató ISMS auditoroknak az információbiztonsági ellenőrzésekről
- ISO 27009 – Nincs kiosztva
- ISO 27010 – Ágazatok és szervezetek közötti kommunikáció szabályozása információbiztonsági szempontból
- ISO 27011:2008 – A telekommunikáció információbiztonsága
- ISO 27012 – Nincs kiosztva
- ISO 27013 – Útmutató az ISO/IEC 27001 és ISO/IEC 20000-1 szabványok integrált bevezetéséhez
- ISO 27014 – Az információbiztonság irányítása
- ISO 27015 – Javaslat a pénzügyi szervezetek és biztosítók információbiztonsági rendszereiről
- ISO 27016 – Információbiztonság irányítása: szervezeti gazdaságtan[1]
- ISO 27017-1 – Nincs kiosztva
- ISO 27017-2 – Útmutató az információbiztonsági kontrollok használatára felhő alapú szolgáltatásoknál
- ISO 27018 – 27030 – Nincs kiosztva
- ISO 27031:2011 – Biztonsági technikák: útmutató az információs és kommunikációs technikák felkészültségéről az üzletfolytonosság megközelítésében
- ISO 27032 – Biztonsági technikák: útmutató a kibervédelemhez
- ISO 27033-1:2009 – Hálózati biztonság: áttekintés és fogalmak
- ISO 27033-2.2 – Hálózati biztonság: hálózati felépítések referencia: fenyegetések, tervezési elvek és ellenőrzések
- ISO 27033-3 – Nincs kiosztva
- ISO 27033-4 – Hálózati biztonság: gatewayekkel[2] összekötött hálózatok közötti biztonságos kommunikáció
- ISO 27033-5 – Hálózati biztonság: VPN[3]-nel összekötött hálózatok közötti biztonságos kommunikáció
- ISO 27033-6 – Hálózati biztonság: biztonságos IP vezeték nélküli hálózat kialakítása
- ISO 27033-6 – Hálózati biztonság: vezeték nélküli rendszerek
- ISO 27034-1:2011 – Alkalmazásbiztonság: áttekintés és alapfogalmak
- ISO 27034-2 – Alkalmazásbiztonság: szervezeti normatív keretrendszer
- ISO 27034-3 – Alkalmazásbiztonság: alkalmazásbiztonsági irányítási folyamatok
- ISO 27034-4 – Alkalmazásbiztonság: alkalmazások biztonságának érvényesítése
- ISO 27034-5 – Alkalmazásbiztonság: protokollok és alkalmazásbiztonsági adatstruktúra
- ISO 27035:2011 – Információbiztonsági incidenskezelés
- ISO 27036-1 – Információbiztonság szállítói kapcsolatokban: áttekintés és alapfogalmak
- ISO 27036-2 – Információbiztonság szállítói kapcsolatokban: általános követelmények
- ISO 27036-3 – Információbiztonság szállítói kapcsolatokban: útmutató ICT (information and communications technology) szállító láncok biztonságához
- ISO 27037 – Útmutató az elektronikus bizonyítékok azonosításához, összegyűjtéséhez, megszerzéséhez és tárolásához
- ISO 27038 – Specifikáció a digitális szerkesztéshez
- ISO 27039 – Behatolás jelző rendszer kiválasztása, bevezetése és működtetése
- ISO 27040 – Biztonsági technikák: háttértárak biztonsága
- ISO 27041 – Útmutató a nyomozási eljárások megfelelő lefolytatásához
- ISO 27042 – Útmutató az elektronikus bizonyítékok analizálásához és bemutatásához

(Folytatjuk)

Otti Csaba *(Óbudai Egyetem, Bánki Donát Kar, Alkalmazott Biometria Intézet, mérnök-közgazdász)* ***– magánbiztonsági szakértő***
Rónaszéki Péter *(ISACA Magyarország Egyesület, elnökségi tag) CISA, CISM, ISO27001LA* ***– információbiztonsági szakértő***

[1] *Ezt a szabvány annak érdekében hozzák létre, hogy az IS szakemberek közös nyelven tudjanak kommunikálni a felső vezetéssel.*

[2] *Gateway: átjáró – Az átjáró feladata az, hogy két hálózat között biztosítsa az átjárhatóságot mind hardver, mind szoftver szempontjából (Tannenbaum)*

[3] *VPN: Virtual Private Network – Virtuális magánhálózat*

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.*