AZ INFORMATIKAI BIZTONSÁG AUDITÁLÁSA

Muha Lajos, *fixx@mail.datanet.hu*
FIXX Informatikai, Kereskedelmi és Szolgáltató Kft.

The most countries in Europe have a well regulated system for accreditation and certification of IT security. This not the case in Hungary. In this presentation we focus on accreditation, which is a formal declaration by the accrediting authority that the IT system is approved to operate at an acceptable level of risk in a particular environment. The certification is the technical evaluation of a system's security features, made as a part of and in support of the accreditation process. Certification establishes the extent to which a system's design and implementation of security features meet a set of security requirements.

1. Bevezetés

A fejlett gazdasággal rendelkezõ országokban a különbözõ szervezetekben megjelenik az *audit* rendszere, amelyet magyarra ellenõrzésként fordíthatunk, de a vizsgálat is helyes kifejezés — igazá ból egyik sem adja vissza a pontos jelentését.

Az audit fogalma a pénzügyi-számviteli területen közismert. Kevésbé ismert azonban, hogy az informatikai rendszerekre vonatkozóan is már régen létezik az auditálás rendszere, az un. IT audit. 1969-ben Los Angeles városában alakították meg az Information System Audit and Control Association-t, amelynek ma 58 országban 140 szervezete és mintegy 14.000 tagja van.

Az informatikai auditálás feladata:

- a fejlesztés alatt álló rendszerek vizsgálata;
- az mûködõ adatfeldolgozó rendszerek ellenõrzése;
- az alkalmazások figyelemmel kisérése;
- a nem informatikai ellenõrzés támogatása.

Hazánkban az informatikai rendszerek teljes körû auditálása még gyerekcipõben jár, hiányzik hozzá a belsõ igény a szervezetekben, nincs elegendõ erre felkészült szakember, és sok esetben a szûkös pénzügyi lehetõségekbõl a fejlesztés és mûködtetés mellett az auditálásra már nem futja. A szervezeteknek azonban védekeznie kell az adatai *bizalmasságának, hitelességének és sértetlenségé nek*, az adatok és az azokat kezelõ rendszerek *funkcionalitásának és rendelkezésre állásának elvesz tése ellen*, különösen, ha azok nagy tömegben számítástechnikai rendszerekben kerülnek feldolgo zásra. Ez egyik oldalról részterülete az informatikai auditálásnak, más szempontból viszont több an nál, hiszen nem csak magát az infor matikai rendszert kell auditálni, hanem a szervezet minden olyan részét, amely a biztonság szempontjából nézve kapcsolatban áll az adatfeldolgozó rendszerrel. Ezt az auditálási tevékenységet nevezzük informatikai biztonsági auditálásnak (IT security audit).

Az informatikai biztonsági auditálás ugyanúgy kettõs belsõ és külsõ audit során valósul meg, mint a bármely más auditálás a szervezetben. A belsõ audit feladata, hogy közvetlenül a szervezet ve zetését támogatva, folyamatosan biztosítsa a szervezet materiális és immateriális értékeinek megõr zését, az adatok pontosságát és megbízhatóságát, a törvényi kötelezettségek, a belsõ szabályozás és a szervezet biztonságpolitikájának összhangját. A külsõ audit feladata kettõs. Egyrészt elfogulatlan, külsõ ellenõrként ellenõrzi és értékeli a informatikai rendszer biztonságát, másrészt vizsgálja a belsõ ellenõrzés tevékenységét is.

Az informatikai biztonsági audit a rendszer eg észére:

— vizsgálja az elõírt és a meglévõ biztonsági szint közötti távolságot és
— ellenõrizze a védelem teljes körûségét és zártságát.

2. Miért szükséges az informatikai biztonsági audit

Nagyon fontos, hogy a rendszer felhasználói megbízzanak az általuk használt rendszer védett ségében, biztonságában, ismerjék annak biztonsági szintjét. Egy valós, mûködõ informatikai rendszer azonban nem pusztán a beszerzett informatikai eszközök összessége, hanem hardver, szoftver, az azokat befoglaló infrastruktúra, a mûködés szabályozása, a felhasználó és az üzemeltetõ személyzet összessége, így a beépített termékek biztonsági szintjébõl még nem következik közvetlenül a rend szeré, bár a rendszer biztonsági szintjének megismeréséhez az ahhoz felhasznált informatikai termé kek biztonsági szintjét is i smerni kell.

Mindehhez azonban szükséges, hogy legyen egy mérce, mellyel összehasonlítható a tervezet vagy mûködtetett rendszer, illetve a mûködtetett vagy a beszerzendõ informatikai termékek bizton sági adottsága. Annak ellenére, hogy ezek vonatkozásában a felhasználók többnyire megbízhatnak a termékek gyártóinak, eladóinak szavában, illetve azokat maguk is kipróbálhatják, mégis valószínû, hogy sok felhasználó szívesen támaszkodik egy független testület el nem kötelezett vizsgálata révén biztosított valamiféle eredményre. A rendszereknek vagy termékeknek az ilyen kiértékeléséhez ob jektív és jól körülhatárolt biztonsági értékelési követelményrendszerre van szükség, illetve egy olyan bizonyítványt kibocsájtó testület létezésére, mely igazolja, hogy a kiértékelést megfelelõ módon haj tották végre. A rendszer biztonsági cé lkitûzéseit a kérdéses rendszer felhasználójának egyedi igényei határozzák meg, míg a termék biztonsági célkitûzései általánosabbak, miáltal az ennek megfelelõ termékek sok hasonló, de nem szükségszerûen azonos védettségi szintû rendszerbe építhetõk be.

Egy rendszer esetében a biztonsági adottságok értékelését fel lehet fogni az informatikai rend szer meghatározott környezetben való használatának hivatalos vizsgálataként is. Ezt a folyamatot *akkreditáció*nak is szokták nevezni. Mielõtt a rendszert egy tervezett cél megvalósítására alkalmas nak minõsítenék, számos tényezõt szükséges mérlegelni:

— szükséges a rendszer által biztosított biztonság garantálása;
— a védelem irányítási szintjéhez való alkalmazkodás;
— a fontos mûszaki, jogi és irányítási követelményeknek való megfelelés;
— a rendszer környezetében érvényesülõ, nem mûszaki jellegû biztonsági intézkedések megbízható mûködésének feltételezése.

3. Informatikai biztonsági követelményrendszer

Az elmúlt idõszakban szerte a világon sok munkát fordítottak az informatikai rendszerek és termékek biztonsági kiértékeléséhez szükséges követelményrendszer felállítására, kifejlesztésére, bár a részt vevõ országok és szervezetek egyedi igényei miatt, néha kissé különbözõ szempontok szerint. Ezek közül a legfontosabb — és sok szempontból más fejlesztések meghatározó alapja is — a Biz tonságos Számítógép Rendszerek Értékelési Kritériuma, melyet általában csak TCSEC-ként, vagy "orange book"-ként szoktak emlegetni. Ezt az Egyesült Államok Védelmi Minisztériuma adja ki és használja termékek minõsítéséhez. Más országok, így az Egyesült Királyság, Németország, Francia ország egyedileg is kidolgozták a saját informatikai biztonsági követelményrendszerüket, azonban az Egyesült Királyság, Franciaország, Hollandia és Németország az ezen a téren folyó munkát, illetve a megoldásra váró feladatokat figyelembe véve arra a következtetésre jutott, hogy a megvalósításhoz koncentrálni kell erejüket, és egységes, összehangolt informatikai biztonsági követelményrend szert kell kidolgozniuk. Az össz ehangolásnak több oka is volt, többek között, hogy létrejöjjön a négy együttmûködõ ország nemzeti bizonylatolási szervezetei által kibocsátandó, egymással azonos értékû

bizonyítvány, melynek végsõ állomása az értékelés eredményének nemzetközi, közös elismerése. Ez a dokumentum az *ITSEC*, az Információ Technológia Biztonsági Értékelési Kritériuma. Ma már az Európai Közösség országaiban ezt a követelményrendszert széles körben elfogadják és használják a potenciális felhasználók és piaci szekt orok.

A fejlett ipari országok, ezen belül is elsõ sorban az EK követelményrendszeréhez való iga zodás szándéka vezette a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottságát abban, hogy az elmúlt évben elkészítse az ITSEC hazai adaptációját, mint a Tárcaközi Bizottság ajánlását, amely az Informatikai Rendszerek Biztonsági Követelményei címmel jelenik meg a közeljövõben. Elõkészü letben van az Informatikai Biztonsági Kézikönyv is, amely már az alapfokú biztonság konkrét meg valósításához gyakorlati útmutatót fog biztosítani. Ezt a követelményrendszert úgy terveztük meg, hogy az — a nemzetközi követelményrendszerekhez hasonlóan — a lehetõ legkisebb szintre csökkentse a ki értékelési ere dmények szubjektív tényezõit.

Az informatikai biztonság területén azonban nem ez volt a kormányzati szféra elsõ megmozdu lása. 1994-ben adta ki az Informatikai Koordinációs Iroda az ITB 8. számú ajánlását, az *Informatikai Biztonsági Módszertani Kézikönyv* et. Ez a dokumentum az informatikai rendszerek — fõleg külsõ — auditálásához nyújt jól használható módszertant. Ez a módszer a német, északrajna-vesztfáliai kormány Informationtechnik Sicherheitshandbuch-ján és a brit kormány által használt CRAMM mód szeren alapul. Ezt a módszertant immár másfél éve használjuk a gyakorlatban, elsõ sorban államigaz gatási szervezetek auditálására, de ezt adaptáltuk a "civil szférára" is.

4. Az auditálás módszere

Az informatikai biztonsági vizsgálat során természetesen szerte a világon számos különbözõ módszertant használnak, azonban ezek mindegyike az un. kockázatelemzésre épül.

Az általunk is használt módszer lényege a következõ:

Interjúk sorozatával megismerjük a rendszer un. reál folyamatait, az azokhoz szükséges adato kat és azt, hogy ezek közül melyek kerülnek feldolgozásra az informatikai rendszerben. A megrende lõvel közösen rögzítjük *a szervezet védelmi céljait* , amelyeknek összhangban kell lenni a jogsz abályi elõírásokkal, a politikai-gazdasági környezet igényeivel. Felmérjük az informatikai rendszer *alkalmazásait és adatait,* meghatározzuk azok *lehetséges kárértékét* az öt alapfenyegetettség, vagyis a bi zalmasság, a hitelesség, a sértetlenség, a funkcionalitás és a rendelkezésre állásnak elvesztése esetén.

Feltérképezzük *a fenyegetett rendszerelemeket* , azok gyenge pontjait, a lehetséges fenyegeté seket és rendszerelemeinek lehetséges kárértékeit az öt alapfenyegetettség vonatkozásában. A rend szerelemeket fenyegetõ károk alapján megállapítjuk a lehetséges fenyegetések révén elõállható lehet séges károkat, azok gyakoriságát. Ezek a kár- és gyakorisági értékpárok mutatják az egyes fenye getések kockázatát. Ha valamely kockázat szintje nem elviselhetõ, akkor azokra megkeressük azt az optimális megoldást, amely a kockázatot lehetõleg az elviselhetõ szintre csökkenti. A megrendelõ igénye esetén a kockázat-menedzselést is elvégezzük, amikor a javasolt intézkedéseket több iteráció ban vizsgáljuk, részben elméletben, részben gyakorlatban arra nézve, hogy milyen mértékben csök kentik az adott fenyegetés kockázatát, milyen kölcsönhatásban vannak más fenyegetésekkel, illetve az azokkal kapcsolatos védelmi intézkedésekre.

Mint érezhetõ ez a módszer csak az informatikai rendszerek auditálására alkalmas, termékek esetében nem használható.

Az informatikai biztonsági audit célja, hogy a vizsgálatot végzõ egy olyan részrehajlásmentes jelentést készíthessen, melyben kijelenti, hogy a szervezet védelmi céljainak az informatikai rendszer védelmi adottságai megfelelnek-e vagy sem. Ez elengedhetetlenné teszi a vizsgálat megrendelõjének (szponzorának) bevonását, szoros együttmûködését. Minél magasabb a megkövetelt biztonsági szint, annál nagyobb szükség van a szponzor bevonására. Az auditálás szponzorai lehetnek a felhasználók vagy akár az eladók is.

Annak érdekében, hogy egy auditálás a lehetõ legkisebb költségkihatással véghezvihetõ legyen, a vizsgálónak szorosan együtt kell mûködni a szponzorral és a tervezõvel vagy a fejlesztõvel.

A szponzornak kell meghatározni azokat a mûködéssel kapcsolatos követelményeket és veszé lyeket, melyekkel a vizsgált rendszer vagy termék esetében számolni kell. Egy rendszer esetében szükséges a rendszer valós mûködési környezetének vizsgálata, miáltal meghatározhatók azon a fontosabb veszélyeztetettségi tényezõk, melyeket figyelembe kell venni. Egy termék esetében meg határozandók a termékkel kapcsolatos veszélyeztetettségi aspektusok. Ideális esetben az auditálást rögtön a fej lesztés elején kezdik.

Feltételezhetõ, hogy idõvel az informatikai iparág szervezetei, a nemzetközi szabványügynökségek, vagy a biztosítók szabványos biztonsági funkcionalitási osztályokat fognak felállítani a termék védettségi szintjéhez rendelve. A termékfejlesztõk, akik nem egy elõre meghatá rozott, special izált piaci részt céloznak meg, illetve nem egy típusú felhasználóban gondolkodnak, az ilyen elõre meghatározott biztonsági funkcionalitási osztályokat jól hasznosíthatják saját termékeik védettségi szintjének tervezéséhez. Ilyen követelményeket ír le a korábban már említett ITB ajánlás, az Informatikai Rendszerek Biztonsági Követelm ényei.

5. Az auditor függetlensége

Az informatikai biztonsági auditorok szerepe sok tekintetben analóg a könyvvizsgálóéval, akinek éppúgy szükséges jó munkakapcsolatot kialakí tani a gazdasági vezetéssel, és aki — sok esetben az elvégzett vizsgálatokat követõen is — használni fogja a belsõ nyilvántartásokat és szabályzókat. Ugyanakkor e személynek vagy szervezetnek is fü ggetlennek, és tényfeltárónak kell maradnia.

Az auditor nem lehet a vizsgált rendszerrel vagy termékkel sem szervezeti, sem gazdasági kap csolatban. A vizsgálót sem közvetlen, sem közvetett módon nem befolyásolhatja senki a vizsgálat so rán. A vizsgáló nem lehet érdekelt abban, hogy a vizsgálat az általa gyártott vagy értékesített termé ket elõnyben részesítse, vagy a konkurens termékeket hátrányba hozza. A rendszer vizsgálata nem irányulhat termék értékesítésre. A függetlenségét a semleges, nem gyártó vagy termék orientált vizsgálati módszertan is biztosítja, amely nem részesít elõnyben terméket, szállítót, felhasználói vagy üzemeltetõi érdekeket. Az auditor nemzetközi és/vagy nemzeti informatikai biztonsági követelmén yrendszer alapján értékel.

Ezért és, hogy a már többször említett követelményrendszernek gyakorlati haszna is legyen a független auditorok gyakorlati ellenõrzõ tevékenységét megfelelõ *képesítéssel rendelkezõ és nemzeti szinten bizonylatolási jogosultsággal felruházott szervezet* nek kell koordinálni. Ez a szervezet járul hozzá a követelményrendszer által meghatározott eljárások lefolytatásához, a *biztonsági osztályba sorolásra* vonatkozó bizonyítványokat bocsát ki, melyek alapja a szabályosan lefolytatott független vizsgálat, feladata továbbá az engedéllyel rendelkezõ kiértékelõ kiválasztása és irányítása.

A nemzeti bizonyítványt kibocsájtó szervezet feladata, felelõssége a hiteles kiértékelési eredmények egységességének biztosítása. Ennek megalapozása már az Informatikai Koordinációs Iroda megrendelésére folyik.