AZ INFORMATIKAI BIZTONSÁG TERVEZÉSI KÉRDÉSEI

Bodlaki Ákos, akos. *bodlaki@fixx.datanet.hu*
FIXX Informatikai, Kereskedelmi és Szolgáltató Kft.

Abstract

In our experiences the planning of IT security systems isn't an everyday practice. Many data owners and users buy a kind of security device prior to analyse the threats and the weak points of their IT system. In this presentation we focus on the planning method and steps to implement a closed, full scoped trusted information system so, that the realization costs of the security system should be kept on the level of the security risks.

1. Bevezetés

Az informatikai rendszerek rohamos terjedésével, a hálózatok világméretûvé szélesedésével egyre nehezebbé válik a biztonság kézbentartása. Mind többen kerülnek kapcsolatba ezekkel a rendszerekkel, így az informatika világában is jelentkezik — a társadalom egyéb területein sajnos már régóta ismert — visszás jelenség, a bûnözés, esetünkben a "fehérgalléros bûnözés". Hozzá kell szoknunk, hogy információs rendszereinket, hálózatainkat nem használhatjuk "önfeledten", mind jobban gondolnunk kell arra, hogy egyre több személy vagy szervezet érdekében áll az informatikai rendszerbe ágyazott érték, az adatok által hordozott információ illetéktelen megszerzése, épségének vagy hitelességének megsértése tudatos megfontolásból vagy egyszerûen "csak" felelõtlen károkozási szándékkal.

Egy informatikai rendszer számtalan pontján és sokféle módon támadható, így — különösen ha az nagyméretû és összetett — a védekezés helye és módja egyáltalán nem kézenfekvõ feladat. A teljeskörû és zárt védelem (mert csak ez hatásos!) létrehozása csak egy átgondolt tervezési folyamat után valósítható meg.

2. Az informatikai biztonság elvi és gyakorlati modellje, a tervezési alapfeladat megfogalmazása

A informatikai biztonság alapproblémájának megfogalmazását legszemléletesebben a játékelmélet segítségével fogalmazhatjuk meg. Az alapfelállás az, hogy a központban áll egy érték, az adatok által hordozott információ, amelyet az egyik oldalról "támadnak", a másik oldalon az információk tulajdonosa pedig védi azt. Mindkét fél egymástól független, egymás számára ismeretlen stratégiával igyekszik megvalósítani támadási, illetve védelmi szándékait. A játékelmélet nyelvén ez a szituáció a "két személyes, nullától különbözõ összegû játékkal" modellezhetõ, amelyben a támadó(ka)t és a védõ(ke)t egyszerûsítéssel egy-egy személy testesíti meg, akik egymás szándékairól semmilyen vagy nagyon hiányos információkkal rendelkeznek. A játék kimenetele mindig nullától különbözõ abban az értelemben, hogy a védõ a sikeres támadással általában jóval többet veszít, mint amit a támadó nyer.

A tervezés feladata egy olyan optimalizálási feladatra vezethetõ vissza, amelyben a cél egy olyan védelmi rendszer kialakítása, amely a hiányosan ismert stratégiával dolgozó támadó ellen a rendszer minden pontján a kockázatokkal arányos védelmet nyújt úgy, hogy közben figyelembe vesszük a védelem kiépítésének költségeit is. Más szóval a kockázatot nem szükséges nullára csökkenteni, mert a költségek a kárértéket is meghaladó értéket érhetnek el. A támadó stratégiája ismeretének hiányában az egyik lehetséges módszer a fenyegetések kockázatának megbecsülése, amely az okozott kárérték és a támadások becsült gyakorisága

szorzatával azonos. Ha a lehetséges kárértékeket és a bekövetkezési gyakoriságokat tartományokra osztjuk, akkor a kapott kockázati mátrixban meghatározhatók azok a kárérték-gyakoriság értékpárok, amelyek alatt a kockázat *"elviselhetõ"*, illetve afelett *"nem elviselhetõ"*, azaz minden esetbe konkrétan mérlegelendõ a kockázat értéke és a csökkentését célzó védelmi intézkedések költségeinek egymáshoz való viszonya. Az optimális megoldás az, ha minimális védelmi költségekkel a maximális kockázatcsökkentést tudjuk elérni. Egy összetett és nagykiterjedésû informatikai rendszerben ez csak a fenyegetések, gyenge pontok alapos felmérése és a kockázatok elemzése után tehetõ meg, amelyek alapján összeállíthatók a védelmi i ntézkedési javaslatok.

A további tervezési lépések ismertetése elõtt röviden bemutatjuk azt a gyakorlati modellt, amely az informatikai biztonsági vizsgálat és tervezés tárgyául szolgál. Ez alapján könnyebben meghatározható lesz az informatikai biztonság fogalma és a tervezési lépések.

A támadás , illetve a védelem alapvetõ tárgya az *adat*, amely az információkat hordozza. A támadások azonban nem közvetlenül érik az adatokat, hanem az azokat "körülvevõ" *rendszerelemek* (pl. a hardver és/vagy szoftver elemeken, a környezeti infrastruktúrán keresztül). A támadás alatt nem csak az adatok bizalmasságát, sértetlenségét, hitelességét veszélyeztetõ akciókat kell érteni, hanem minden olyan fenyegetést is, amely a rendszer megbízható mûködését, ezáltal az adatok rendelkezésre állását és a funkcionális követelményeknek megfelelõ felhasználásukat veszélyezteti

Az adatot mint a támadások alapvetõ célját "belülrõl-kifelé" a következõ rendszerelemek veszik k örül:

- szoftver rendszer,
- hardver rendszer,
- kommunikációs (hálózati) rendszerek
- adathordozók,
- dokumentumok és dokumentáció,
- az informatikai rendszer fizikai környezete és infrastruktúrája,
- személyi környezet (külsõ és belsõ).

E rendszerelemekre különbözõ fenyegetések hatnak, amelyek a rendszerelemek meghatározott láncán keresztül az adatokat veszélyeztetik. Így a védelmi intézkedések is közvetlenül a rendszerelemekhez kapcsolódnak. Ha az összes fenyegetésnek kitett rendszerelemet a kockázattal arányosan kiépített védelemmel látjuk el úgy, hogy közben figyelembe vesszük a különbözõ védelmi intézkedések sokszor egymást erõsítõ hatását is, akkor az informatikai biztonságot olyan szintre emeltük, amelynél az adott valószínûségû támadások mellett a káresemények bekövetkezésének valószínûsége lényegesen alacsonyabb, azaz a kockázat elviselhetõ mértékû, de soha nem nulla. Száz százalékosan biztos védelmi rendszer nincs. Az elviselhetõ kockázat mértékét minden egyes konkrét vizsgálati esetben az adatok érzékenységét, az informatikai rendszer és környezetének kialakítását, valamint a meglevõ védelem szintjét figyelembe véve kell kialakítani. Ez a védelmi rendszer tervezésének egyik kiinduló kulcsparamétere, amely csak alapos biztonsági vizsgálattal becsülhetõ meg.

3. Az információ és az informatikai biztonság fogalma

Az információ biztonságot egy teljeskörû, zárt, a kockázatokkal arányos védelem biztosítja a hagyományosan és elektronikusan kezelt és tárolt információk körében.

Ezen belül az informatikai biztonság csak az informatikai rendszer által kezelt és tárolt adatok által hordozott információk körére vonatkozik és vizsgálódási területe magukon az adatokon kívül magába foglalja korábban felsorolt összes rendszerelemet, amelyek valamilyen kapcsolatban vannak az adatokkal. Az összes

lehetséges rendszerelemre ható fenyegetések elemzése az egyik legfõbb biztosítéka a kialakítandó védelem teljeskörûségének.

A rendszerelemeken keresztül hatnak egyrészt azok az alapfenyegetések (a bizalmasság, a hitelesség, illetve a sértetlenség elvesztése), amelyek miatt az adatok által hordozott információk védelmét biztosítani kell, másrészt azok az alapfenyegetések (a rendelkezésre állás és a funkcionalitás elvesztése), amelyek az informatikai rendszer megbízható mûködését erõsítõ intézkedéseket igénylik. Sok esetben az informatikai rendszer által kezelt információk védelme azonos értelmezés alá esik az informatikai biztonság fogalmával. Ez egy szûkített értelmezés, mert az adatok rendelkezésre állásának és a hozzájuk kapcsolódó funkcionalitásának biztosítása is az informatikai biztonság tárgykörébe esik.

Egy másik vizsgálódási szempont rendszer — a védelmi területek — szerint az informatikai biztonság fogalomköre lefedi a fizikai, a logikai és az adminisztratív védelmek területét. A három területen meghozott intézkedések együttese a másik biztosítéka a teljeskörûségnek és a zártságnak.

4. Az informatikai biztonság és más társterületek kapcsolata

Az informatikai biztonsággal kapcsolatban gyakran említésre kerülnek más diszciplínák, mint pl. a hagyományos biztonság, a minõségbiztosítás, az informatikai rendszerek auditálása, jogtudomány. E fogalmi körök pontos tisztázása egy másik elõadás anyagát tehetnék ki. Itt csak nagyon röviden "tesszük helyre" az informatikai biztonságot tudományterületek viszonylatában.

Az informatikai biztonsághoz képest az informatikai rendszerek auditálása (IT audit) szélesebb területet ölel fel. Az informatikai biztonsági vizsgálat (IT security audit) az IT audit része. A jogtudományhoz az informatikai biztonság elsõsorban az adminisztratív szabályozások területén kapcsolódik, egyrészt az érvényben levõ jogszabályok — fõleg az állam- és a szolgálati, az üzleti és a banktitok, illetve a személyes adatok védelme —, tekintetében, másrészt a szervezetek helyi szabályozási rendszerének kialakításában. A hagyományos biztonság elemei az informatikai rendszerek fizikai védelmében jelennek meg, míg az adatminõség biztosítása az adatok sértetlenségének, hitelességének, rendelkezésre állásának és funkcionalitásának biztosítása területén jelentkezik. Még tovább lehetne folytatni olyan fogalmak felsorolását, mint az informatikai rendszerek tervezési és fejlesztési módszerei, a projekt menedzsment, a beszerzési politika, stb., amelyek valamilyen vonatkozásban mind kapcsolódnak az informatikai bizto nsághoz.

5. Az informatikai biztonság tervezése

A rendszer tervezésének megkezdése elõtt — különösen nagy és összetett szervezeteknél — szükséges egy informatikai biztonsági koncepció, ezen belül egy biztonság politika kialakítása, amelyek megfogalmazzák azokat az alapelveket, amelyeket a biztonsági rendszer tervezése és megval ósítása során be kell tartani.

Az informatikai biztonsági koncepció keretében:

— meghatározandók az informatikai biztonság érvényesítési területei *életciklus* és *alkalmazási tartomány* dimenziókban.

Az életciklus dimenzió lefedi az informatikai rendszer:

- tervezési,
- fejlesztési,
- bevezetési,
- üzemeltetési,
- megszüntetési vagy rekonstrukciós idõszakát.

A másik dimenzióban behatárolandók a szervezet mûködése és tevékenysége szempontjából kritikus alkalmazások és adatcsoport típusok, figyelembevéve a mûködési területeket, a szervezeti struktúrát, a pénzintézmények állapotát és típusát, a feldolgozottság szintjét.

— A fentiek ismeretében meghatározandók az informatikai biztonság területén érvényesítendõ hatályos jogszabályok és kialakítandó belsõ szabályozások.

— Meghatározandók az alkalmazások és adatcsoport típusok veszélyeztetettségi és védelmi igény szintjei, valamint a releváns alapfenyegetések és védelmi célkitûzések szintenként. Az ezek alapján differenciált adatcsoportokhoz meghatározandók a kapcsolódó fizikai és logikai biztonsági tartományok és ezek biztonsági osztálybasorolása. Ezek alapján lesznek majd kialakíthatók az egyes biztonsági osztályok követelményrendszere.

— A fizikai és a logikai biztonsági tartományok és osztálybasorolásuk ismeretében kialakítandó mindegyik tartományra az a *biztonságpolitika*, amely meghatározza az fizikai, illetve a logikai értelemben vett azonosítási és hitelesítési funkciók, hozzáférési, ellenõrzési jogok, valamint az ezeket gyakorló személyek szerepköre közötti összefüggéseket. *Ez lesz az adott szervezet egészét átfogó biztonsági politika*, amely alapján az egyes konkrét esetekben, alkalmazásoknál egységesen és gyakorlati szinten kialakítható lesz az azonosítási és hitelesítési, a hozzáférés jogosultság szabályozó és a biztonsági naplózási rendszer.

— Kialakítandók az informatikai biztonsággal kapcsolatos menedzselési, tervezési, beruházási, üzemeltetési és ellenõrzési funkciók, valamint a vezetési hierarchia és a megfelelõ szervezeti egységek feladat, felelõsség és komptencia köre ezen a területen. Példaképpen megemlítjük, hogy a logikai védelmi rendszer tervezésével és megvalósításával kapcsolatos szabályozásnak biztosítania kell, hogy a védelmi rendszer az adott informatikai rendszer — legyen az infrastruktúra vagy alkalmazás szintû — tervezési és megvalósítási projektjében, integráltan történjék meg.

— Kialakítandó a vész-, illetve katasztrófa megelõzési és elhárítási koncepció, amelynek keretében ki kell térni azokra az elvekre és intézkedés csoportokra, amelyeket követni kell a vész-, illetve katasztrófa megelõzés, bekövetkezés és a normál állapot visszaállítás idõszakában.

A következõ lépésben kidolgozandó az *informatikai biztonsági stratégia*, amely a biztonsági koncepcióban megfogalmazott célkitûzések megvalósítási módszerét és érvényesítési módját deklarálja olyan módon, hogy egy jövõkép (*hova akarunk eljutni*) kialakítása után a jelenlegi helyzet értékelésébõl kiindulva (*honnan indulunk*) módszert, követelményeket, feltétel- és eszközrendszert, valamint intézkedési tervet javasol a jövõkép elérésére (*milyen úton érjük el a célt*).

Ennek keretében:

— röviden be kell mutatni a jelenlegi informatikai rendszert és fel kell vázolni a teljes informatikai biztonsági rendszer tervezett jövõképét,

— kiválasztásra és elhatárolásra kerülnek azokat a területek, amelyeken a biztonsági rendszereket ki kell alakítani és az intézkedéseket kell érvényesíteni,

— a koncepcióban meghatározott osztálybasorolás figyelembe vételével körvonalazni kell a minimális biztonsági követelményeket,

— meghatározandó a biztonsági tervezés módszere,

— meg kell határozni az intézményre vonatkozó biztonsági rendszer megvalósításának prioritásait és ütemezését a fizikai, a logikai és az adminisztratív védelem területein, figyelembevéve a finanszírozási és humánerõforrás feltételeket azzal a célkitûzéssel, hogy a jövõképben megfogalmazott informatikai rendszerre *zárt és teljes körû védelmi rendszer* alakuljon ki,

— meg kell határozni a követhetõség és a menedzselhetõség követelményeit, valamint a felügyelet és az ellenõrzés rendszerét,

— a fentiek ismeretében konkrétan meghatározandók az informatikai biztonsággal kapcsolatos feladat, felelõsség és kompetencia körök szervezeti egység és személyi szinten.

Az informatikai biztonsági koncepciónak integráns részének kell lennie az intézmény mûködési és globális biztonsági koncepciójának. Az informatikai biztonsági stratégiának összhangot kell képeznie a szervezet informatikai stratégiájával. Mindkét dokumentumnak ki kell szolgálnia a szervezet üzleti stratégiai célkitûzéseit. Ez egyúttal azt is jelenti, hogy rövid- és hosszútávra szól.

Egy átfogó biztonsági vizsgálat elvégzése, valamint az informatikai biztonsági koncepció és a stratégia kialakítása után megvannak azok a szakmai feltételek és vezetõi eltökéltség, hogy a védelmi rendszer tervezése megkezdõdhessék. Ha ez egy nagyobb alkalmazás megvalósításával egybeesik, akkor feltétlenül a projekt szerves részeként, azzal egyidõben kell elvégezni. A felhasználói rendszer elkészítése utáni védelmi rendszer tervezés és kialakítás drágább és kevésbé hatékony megoldást eredményez.

A védelmi rendszer fõbb tervezési lépései:

— a biztonsági koncepcióban meghatározott elveknek megfelelõen az egyes fizikai, illetve logikai biztonsági területek biztonsági osztálybasorolása alapján a védelmi követelmények meghatározása biztonsági területenként,
— az alkalmazói szoftver termékválasztásnál a termék védelmi funkcióinak vagy rendszerének értékelése a biztonsági osztály követelményei figyelembe vételével,
— a megvalósítandó fizikai és a logikai biztonsági funkciók meghatározása, az adminisztratív szabályozásokra vonatkozó elképzelés kialakítása,
— a fizikai és a logikai védelmi rendszertervek elkészítés, amelyen belül:
    — a fizikai biztonsági követelmények és funkciók, valamint a szóba jöhetõ eszközök jellemzõinek ismeretében egy fizikai védelmi rendszerterv elkészítése,
    — az eszközök és szállítók kiválasztása,
    — a biztonsági politika gyakorlati értelmezésével logikai védelmi rendszer megtervez és:
        — a biztonsági osztályok és ezen belül a logikai biztonsági tartományok konkrét értelmezése az alkalmazás által kezelt adatcsoportok biztonsági elemzése alapján,
        — az azonosítási és hitelesítési rendszer (user id., password) meghatározása és összerendelésük az alkalmazással, annak alrendszereivel,
        — a szerepkörök és az adatcsoportok közötti hozzáférés jogosultsági mátrix meghatározása,
        — a naplózási rendszer megtervezése a biztonsági követelmények alapján és a szoftver termék által biztosított lehetõségek figyelembe vételével.

    A logikai védelmi rendszert olyanra kell tervezni, hogy biztosítsa a biztonsági osztálynak megfelelõ védelmet, ugyanakkor ne tegye feleslegesen körülményessé az alkalmazói funkciók kezelését és védelmi funkciók végrehajtása ne okozzon 10%-nál több terhelést. A tervezés egyben a legfontosabb garanciája annak, hogy a biztonsági koncepció és a politika teljeskörûen érvényesüljön a szervezet teljes informatikai rendsz erében minden alkalmazás esetében.
— a védelmi funkciók implementációja a rendszerterv alapján,
— az adminisztratív szabályozások (pl. Informatikai Biztonsági Szabályzat, Adatkezelési Szabályzat) elkészítése,
— a védelmi rendszer tesztelése.

A védelmi rendszer tesztelés történhet mesterségesen elõállított feltételek mellett, de megfontolásra tartjuk érdemesnek a valóságos támadási szituációkat jobban szimuláló ún. megbízásos betörések alkalmazását, amellyel a fizikai, a logikai és az adminisztratív védelem együttesének hatékon ysága tesztelhetõ.