

Betörési tesztek feketén-fehéren

Ahhoz, hogy egy IT-biztonsági audit eredményes és hatékony legyen, a megrendelőnek is aktívan részt kell vennie benne az elejétől fogva – állítja a Stratis tanácsadója. Minden betörési teszt a felszínre hoz olyan problémákat is, amelyek minimális ráfordítással, rövid idő alatt orvosolhatók, és jelentősen csökkenthetik a biztonsági fenyegetettséget.

Gyakran az informatikai biztonsági vizsgálatok megrendelői sincsenek tisztában azzal, hogy milyen eredményt várhatnak egy biztonsági audittól. Az is sokszor meglepetésként éri őket, hogy az IT-biztonsági auditra való felkészülésben nem csupán a külsős tanácsadónak, hanem a megrendelőnek is részt kell vennie, már a tervezési fázistól kezdve – hívta fel a figyelmet Kovács Zsombor, a Stratis Vezetői és Informatikai Tanácsadó Kft. munkatársa, akivel a biztonsági audittal kapcsolatos megrendelői, illetve tanácsadói feladatokról beszélgettünk. A megrendelőnek már a tanácsadóval való első egyeztetéseken érdemes tisztában lennie azzal, hogy milyen körre – mely telephelyekre, hálózati szegmensekre, illetve informatikai rendszerekre – kiterjedően kell elvégezni a vizsgálatokat. Általánosan igaz, hogy minél kiterjedtebb a hatókör, annál hosszabb ideig tartanak és annál költségesebbek a vizsgálatok, viszont az audit csak úgy tudja a kívánt értéket adni a megrendelőnek, ha az IT-infrastruktúra fontos üzleti információit, szolgáltatásait lefedi, és az egész a megrendelő számára „személyre van szabva”.

A feladatok tisztázása érdekében érdemes előzetesen szót ejteni a betörési tesztek jellemző típusairól. *White-box* típusú tesztelés során a megrendelő „kiteríti lapjait”, azaz átad minden, az érintett rendszerekkel, eszközökkel kapcsolatos dokumentációt, a tanácsadó pedig az előre megállapodott módszerekkel, eszközökkel méri fel a rendszer lehetséges sérülékenységeit. *Black-box* tesztelés során a tanácsadók nem kapnak több információt a megrendelőtől, mint amennyi a vizsgálatok megindításához feltétlenül szükséges; webalkalmazások *black-box* vizsgálatok ilyen információ például az alkalmazás URL-je. A *black-box* tesztelés jól szimulálja az internetről érkező külsős támadást; ekkor a megbízó üzemetlenül dolgozó alkalmazottjainak többnyire nincs előzetes tudomásuk a vizsgálatokról. A *gray-box* tesztelés során egy belső munkatárs által képviselt fenyegetést vizsgálnak, olyanét, akinek van vala-

milyen mértékű információja, illetve hozzáférése az IT-rendszerekhez, ugyanakkor nem tud teljes körű információhoz jutni velük kapcsolatban. Jellemző megközelítés, hogy a *black-box* vizsgálatokat telephelyen történő *white-box* tesztek követik, amelyek során az auditorok áttekintik az üzemeltetés munkatársaival a külső vizsgálatok során keletkezett naplóbejegyzéseket, felmérve, hogy az üzemeltetési folyamatok és az infrastruktúra milyen mértékben képesek jelezni az internet felől érkező, célzott támadásokat.

FOLYAMATOSAN FRISÍTETT TUDÁS

A biztonsági területen tevékenykedő tanácsadók feladatairól szólva Kovács Zsombor elmondta: az audit előtt a tanácsadónak tisztába kell jönnie azzal, hogy milyen eszközöket használhat (és nem használhat) a vizsgálatok elvégzéséhez. A megrendelővel kötött szerződésben emellett rögzítenie kell azt is, hogy a biztonsági audit során bekövetkező esetleges szolgáltatásleállítás vagy -lassulás befér-e a „játékszabályokba”. Jó megoldás, ha a megrendelő kijelöl egy kapcsolattartót, aki különösen a *black-box* tesztelésnél lehet kiténtette szerepe, hiszen ő rögtön értesíthető, amennyiben valamilyen kritikus biztonsági rést fedeznek fel a vizsgált rendszerben, amely működő, produktív rendszerek kompromittálásához vezethet.

Bár az esetek többségében standard eszközparkkal végzik a vizsgálatot, a független biztonsági szakembereknek folyamatosan frissíteniük kell tudásukat, hiszen mindennap újabb és újabb fenyegetések, sebezhetőségek kerülnek napvilágra, amelyek kihasználására rendszerint rövid időn belül megjelennek az interneten a sok esetben már kevés informatikai tudással is használható támadóeszközök. A tanácsadónak ezért naprakészen követniük kell a forrásokat, hogy a következő megrendelésnél már ezen (akár alig néhány napja ismert) sebezhetőségek is napvilágra kerülhessenek. A gyakorlati ismeretek naprakészen tartására komolyabb biztonsági tanácsadó cégek házon belüli tesztlabor, „homokozót”

szoktak kialakítani, ahol kockázat nélkül kipróbálhatják az újfajta eszközöket.

A vizsgálati terv elkészítése során a tanácsadónak figyelembe kell vennie a megrendelő szervezet környezetét, az adott iparágra és a konkrét cégre jellemző vállalati kultúrát és a használt infrastruktúra elemeit – ez különösen az olyan szimulációknál lényeges, ahol belső kollégák által jelentett fenyegetést modelleznek. A megrendelőnek és a tanácsadónak ezért már az elején tisztázni kell a szabályokat, és meg kell állapodniuk abban, hogy milyen motiváltságú és tudású támadót feltételeznek a vizsgálati helyzet kialakítása során.

NAGY EREDMÉNYEK, KIS RÁFORDÍTÁSSAL

A vizsgálat végén elkészített jelentés minden esetben tartalmaz kockázatelemzést, amelyben a megrendelő más, nem informatikai szakemberei számára is érthető formában összegzik az üzleti kockázatokat és a feltárt sebezhetőségeket. A tapasztalt problémák sok esetben nem is informatikai jellegű okokra vezethetők vissza (így például gondot okozhat a jogosultságkezelési szabályozás hiánya). A jelentés a kockázatok hatása, bekövetkezési valószínűsége és a megoldás erőforrásigénye alapján több területre bontva tartalmaz javaslatokat, amelyek alapján ki tudják választani a megrendelő üzleti döntéshozói, hogy melyek a kis befektetéssel hamar megtehető, és melyek a hosszabb távon megvalósítható, ám költségesebb intézkedések.

A vizsgálatok olyan problémákat is szoktak a felszínre hozni, amelyek minimális ráfordítással rövid idő alatt orvosolhatók, és jelentős mértékben csökkenthetik a biztonsági fenyegetettséget (jellemzően ilyen a vizsgált rendszerekben „ott felejtett”, és az audit során feltárt szolgáltatások leállítás). Sokszor előfordul az is, hogy a vizsgált szervezetnek vannak biztonsági eszközei, de nem használja őket megfelelően – így például a hálózati switch-ekbe (kapcsolókba) beépített, de addig nem használt tűzfalfunkciók használatbavételével jelentősen csökkenthető a szolgáltatások és üzleti adatok fenyegetettsége – mutatott rá Kovács Zsombor.

NINCS JÓ ÉS ROSSZ SZABÁLYOZÁS

Az informatikai infrastruktúra biztonságát két tényező befolyásolja: a rendszerek konkrét technikai beállításai mellett

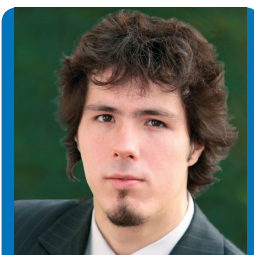
legalább olyan fontos szerep jut a működtetési, fenntartási folyamatoknak, amelyek biztonságáról szabályozással lehet gondoskodni.

Az informatikai szabályozás megalkotásánál nincsenek általános jó és rossz szabályok, azaz a szabályzatok csak akkor láthatják el megfelelően feladatukat, ha a felmerülő kockázatokra és a várható előnyökre való tekintettel, tudatos döntések eredményeképp alkották meg őket. Fontos szem előtt tartani azt is, hogy a szabályzatok életútja nem ér véget az elkészítésükkel, hanem folyamatos aktualizálással kell naprakészen tartani őket. A megrendelőnek azzal is tisztában kell lennie a biztonsági folyamatok kialakításakor, hogy informatikai rendszerében hol helyezkednek el a védendő üzleti információk; ez az IT-biztonsági audit megtervezéséhez is támpontul szolgál – hangsúlyozta a szakértő.

Gyakran elkövetik azt a hibát a szervezetek, hogy a biztonsági intézkedéseket kampányszerűen – általában egy biztonsági audit eredményei ismeretében – végzik el, és ezt követően azt gondolják, hogy a feladat itt véget is ért, ezáltal egyfajta hamis biztonságérzetben működnek tovább. Ezzel szemben a biztonsági intézkedéseket folyamatosan, a standard működési folyamatokba beillesztve kell megtenni – figyelmeztetett a Stratis tanácsadója. Másrészt elsőre az is magától értetődőnek hangzik, hogy a tesztek tanulságait, az auditorok javaslatait érdemes figyelembe vennie a megrendelőnek, de a jelentés átvétele után sokszor figyelmen kívül hagyják a javaslatokat, és a feltárt konkrét technikai sérülékenységek beforozásain túlmutató folyamathelyi hiányosságokat nem, vagy csak részben szüntetik meg.

A biztonsági auditot megrendelő általában tudatosnak tekinthető biztonsági szempontból, hiszen éppen a biztonsági kockázatok szándékos felderítése céljából kérnek fel külső auditort. A biztonsági tudatosságnak azonban már a rendszerek tervezésekor és az őket működtető folyamatok kialakításakor is szerepet kell kapnia, hiszen utólag sokszor nehéz és drága lehet egy sérülékeny rendszer megerősítése.

A tervezési és üzemeltetési folyamatok biztonsági szempontból egyik legfontosabb sarokköve a megfelelően felépített és átgondolt módszertan. A tervezéshez jó támpontot adhatnak az elterjedt nemzetközi ajánlások, mint például a Common Criteria. Az ajánlások konkrét javaslatai és a mögöttük húzódó koncepció szem előtt tartásával kialakított fejlesztési, üzemeltetési folyamatok nemcsak a technikai sebezhetőségek számát csökkentik, hanem proaktívabbá, felkészültebbé teszik az egész szervezetet biztonsági szempontból – hangsúlyozta a tanácsadó.



Kovács Zsombor
tanácsadó
Stratis