Mit jelent etikus hackernek lenni?

Az utóbbi időben egyre többet lehet olvasni, illetve hallani arról, hogy egy hacker sikeresen feltörte xy vállalat informatikai rendszerét, esetleg bizalmas információkat szerzett meg onnan.
A kiberbűnözés térhódításával a hackertámadások száma is folyamatosan növekszik, éppen ezért egy vállalat vagy egy intézmény esetében már az informatikai rendszer kialakítása során fel kell mérni a lehetséges kockázatokat. Bár a biztonság megteremtése pénzügyi szempontból komoly kiadásokat jelent az üzemeltetők számára, ugyanakkor a rosszindulatú hackerek akár a védelemre fordított összeg többszörösét meghaladó károkat is okozhatnak egy-egy támadás alkalmával.

Külföldön már bevett gyakorlat, de Magyarországon is egyre nagyobb az igény arra, hogy a számítógépes hálózatok biztonságát etikus, más néven fehérkalapos (white-hat) hackerek teszteljék. Az etikus hackerek olyan kiemelt tudással rendelkező informatikai szakemberek, akik tudásukat arra használják fel, hogy megbízás alapján vagy állandó jelleggel biztonsági hibákra világítsanak rá, ezáltal elkerülve és megelőzve a feketekalapos (black-hat) hackerek betörési kísérleteit.
Fontos megjegyezni, hogy egy etikus hacker ugyanazokat az eszközöket és módszereket használja, mint egy rosszindulatú, a célja viszont nem a károkozás, hanem a hiba meglétének bizonyítása, méghozzá olyan módon, hogy azt csak a megbízója felé kommunikálja.
Ezzel szemben a „black-hat" hackerek jellemzője, hogy tudásukkal visszaélve, jogosulatlanul törnek be számítógépes-hálózatokba, a sikeres behatolást követően pedig nem értesítik az üzemeltetőket, hanem igyekeznek saját céljaikra felhasználni az illegálisan megszerzett információkat (pl. a dark weben kínálják eladásra a kinyert felhasználóneveket és jelszavakat).

A jelenlegi, mondhatni egyre inkább ellenséges informatikai biztonsági környezetben várhatóan még inkább szükség lesz olyan etikus hackinggel foglalkozó szakemberekre, akik tisztában vannak a vállalati rendszerek sebezhetőségeivel és tanácsot tudnak adni a legkülönbözőbb támadások elhárításának módjairól, ebből kifolyólag érhető, hogy napjainkra az etikus hackelés, mint professzionális foglalkozás is elfogadottá vált.
A fogalmat elterjesztő International Council of Electronic Commerce Consultants (EC-Council) módszertana alapján tartott tanfolyamok elvégzését követően az utóbbi években világszerte több tízezer IT szakember tett sikeres vizsgát etikus hackelésből (Certified Etical Hacker - CEH).

Ma már számos etikus hackeléssel foglalkozó, illetve sérülékenységvizsgálati szolgáltatást nyújtó cég létezik a hazai piacon is, akik az informatikai rendszer gyenge pontjainak feltárása által átfogóbb képet tudnak adni a vizsgálat alá vont rendszer aktuális állapotáról, egyúttal a felmerült hiányosságok, biztonsági rések kijavítására javaslatokat is tesznek a megrendelők számára.

Az állami szféra vonatkozásában a Nemzeti Kibervédelmi Intézeten belül működő Kormányzati Eseménykezelő Központ (GovCERT) végez sérülékenységvizsgálatot az erre szakosodott etikus hacker kollégák bevonásával.