Eltűnnek a jövőben az IT-biztonsági szakemberek?

Az ipari forradalom óta létező aggály, hogy a technológia fejlődésével bizonyos feladatkörök és szakemberek helyét gépek veszik át. Napjaink robbanásszerű modernizációja mellett szinte minden munkakörrel kapcsolatban felmerül ez a kérdés.

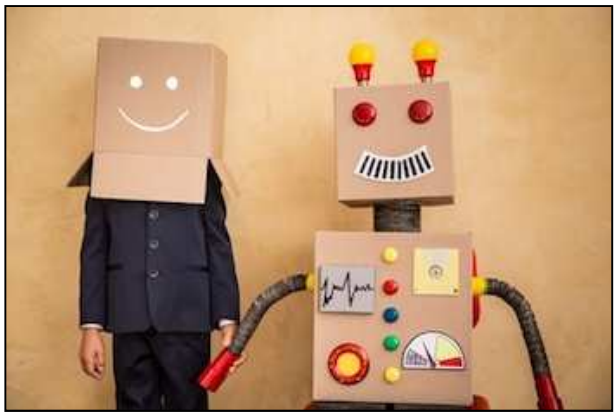
A NetIQ szakértői azt járták körbe, vajon megalapozott-e ez a félelem az IT-biztonsági szakemberek esetében.

Az elmúlt években egyre több szakértő figyelmeztet arra, hogy az automatizáció számos munkahelyet megszüntethet, ez a félelem azonban napjainkban leggyakrabban a gyártás területével kapcsolatban merül fel, méghozzá jó okkal. Az *International Federation of Robotics* adatai szerint az autógyártásban működik a legtöbb robot, a gépek 40 százalékát ebben a szektorban alkalmazzák világszerte.

Egyelőre tehát leginkább a gyári dolgozókat fenyegeti az, hogy egy robot elveszi a munkájukat, de a jövőben bármelyik ágazat szakemberei veszélyben érezhetik a megélhetésüket. Erre nemrégiben a *Gartner* egyik szakértője mutatott rá a következő címmel közzétett blogposztjában: „Milyen robotbiztos szakmát válasszon a gyermekem?”. A bejegyzés végkövetkeztetése szerint nincs általános válasz a kérdésre, hiszen a technológia bármit megváltoztathat. Míg a gyártási területeken a robotok térnyerése figyelhető meg, a szellemi munka esetében a mesterséges intelligenciák gyors fejlődése jelzi előre, hogy a jövőben lecserélhetők lehetnek a szakértők. Erre az eshetőségre olyan szakemberek, tudósok és üzletemberek is figyelmeztetnek, mint *Stephen Hawking, Elon Musk* vagy *Jonathan Rosenberg*, a Google korábbi alelnöke.

A „gépek” térnyerése a kibervédelemben (és -támadásokban)

Az olyan szakemberek számára, akik az információk biztonságával, felügyeletével és tárolásával foglalkoznak, többnyire elképzelhetetlennek tűnik, hogy munkájukat automatizálják. Miközben egyre több előrejelzés mutat rá arra, hogy a mesterséges intelligenciát és a gépi tanulást széles körben fogják alkalmazni az IT-biztonság terén. A Gartner friss jóslatai szerint 2020-ra például a penetrációs tesztek 10 százalékát már szintén gépi tanulást alkalmazó, okos rendszerek fogják végezni, míg ez a szám 2016-ban még 0% volt. A folyamat érthető, hiszen folyamatosan nő a támadók és a támadási felületek száma, ezért a vállalatok és az állami szervezetek, kormányzatok is keresik a megoldásokat, amiben hathatós segítség lehet a mesterséges intelligencia.



A másik oldal természetesen ugyanúgy kihasználhatja az AI előnyeit. Egy, az AI és a kiberbiztonság kapcsolatát vizsgáló szakértő például arra figyelmeztet, hogy az AI előnyeit kihasználó támadások következtében várhatóan robbanásszerűen nő a különféle incidensek száma, beleértve a hálózatok feltörését, a személyes adatok ellopását és az intelligens vírusok járványszerű terjedését.

A mesterséges intelligenciában az a veszélyes, hogy - mint ahogyan bármely technológiát - jó és rossz célokra egyaránt fel lehet használni. Egy programozó szándékosan vagy akár véletlenül is okozhat valamilyen hibát, amely kettős ügynökké változtatja a "védőt", és ezzel veszélynek teszi ki az adatokat, vagy lehetővé teszi, hogy mások átvegyék az irányítást kívülről. További veszélyt rejthet, ha az AI a tulajdonosai ellen fordul. Az egyelőre még csak sci-fikben létező forgatókönyv valódi aggodalomra ad okot, ahogy egyre több rendszer és feladat kapcsolódik mesterséges intelligenciához.

Felkészülés az automatizált jövőre

Akár tetszik, akár nem, az automatizálás egyre nagyobb szerepet játszik az IT-biztonságban. Az ilyen jellegű megoldások már most is komoly előnyt biztosítanak a támadások észlelésében és elhárításában. A NetIQ Sentinel biztonsági információ- és eseménykezelő termék segítségével például akár több ezer szerver, hálózati eszköz és szoftver figyelhető meg hatékonyan, míg a manuálisan, emberi munkával végzett megfigyelés és kockázatelemzés már kis számú monitorozott eszköz esetén is óriási teher, és számos hibalehetőséget is magában rejt. A megoldás szükség esetén képes automatikus válaszlépéseket is tenni, hogy azonnal elhárítsa a veszélyeket.

Az automatizálás tehát hatékonyabb működést tesz lehetővé, ennek következtében bizonyos szakemberek munkájára kevésbé vagy egyáltalán nem lesz szükség. Ugyanakkor a változás új feladatköröket és munkahelyeket teremt, amelyek betöltői az automatizált folyamatok szakértői lesznek. Elképzelhető például, hogy a későbbiekben minden nagyobb vállalati IT-biztonsági csapatban szükség lesz AI-biztonsági szakemberre.

Nem valószínű tehát, hogy a jövőben nélkülöznünk kéne az IT-biztonsági szakembereket, de a szerepek átalakulnak, ahogy egyre nagyobb felelősséget kapnak a mesterséges intelligenciák az adatok védelmében. Napjainkban az a legnagyobb kihívás, hogy olyan szaktudást szerezzünk, amely segít az átalakulás követésében, illetve elősegítésében.

Forrás: **https://computerworld.hu/ceginfo/eltunnek-jovoben-it-biztonsagi-szakemberek-237154.html**

Válogatta: Fonyó Istvánné