Mesterséges intelligencia segíthet, hogy a globális IT munkaerőhiány okozta biztonsági réseket betömjék a vállalatok

Miközben becslések szerint a hackerek az évtized végére évi 5 milliárd személyes adatot is ellophatnak a legnagyobb vállalatoktól, pénzügyi és távközlési szolgáltatóktól, kormányzati szervektől, addig a piacról 2 millió IT biztonsági szakember is hiányozhat. Az IBM legújabb fejlesztései ezen a területen is segíthetnek a mesterséges intelligencia (MI) és gépi tanulás alkalmazásával építve fel olyan kibervédelmi rendszereket, amelyek XXI. századi robotzsaruként támogatják az IT szakemberek munkáját, felismerve és kivédve kibertámadásokat.

A dolgok internete a kibertámadások új veszélyzónája

Előrejelzések szerint az évtized végére a dolgok internetén (IoT) megtámadható eszközök száma meghaladja majd a 25 milliárdot.

Rehus Péter, az IBM Magyarország Kft. vezetője szerint minden egyes ilyen hálózatra kötött eszköz olyan gyenge láncszem lehet, amely megfelelő védelmi rendszer nélkül alkalmat adhat a támadóknak, hogy behatoljanak akár kritikus területekre is. „Minél több eszközzel csatlakozunk egy hálózathoz, annál több felületet adunk biztonsági rések kialakulására. Miközben a kiberbűnözők egyre szervezettebbé és fejlettebbé válnak, a hagyományos szabályalapú biztonsági rendszerek nehezen képesek kezelni a komplex támadásokat és a gyorsan változó üzleti környezet kihívásait. Egy biztonsági rendszer hatékonysága pedig éppen attól függ, mennyire gyorsan és hatékonyan képes azonosítani egy fenyegetést. Ebben jelenthet áttörést a hatalmas adatbázisokat feldolgozni képes, tanítható kognitív biztonsági rendszerek alkalmazása” – összegzi Rehus Péter. Fontos terület a védelem hatékonyabbá tétele, mert becslések szerint a kiberbűnözés okozta károk 2021-re elérhetik a 6 billió dollárt, miközben a fenyegetés elkerülésére a cégek várhatóan 1 billió dollárt költenek.

Gyorstanuló robotzsaruk segíthetik az IT szakembereket

Kevin Skapinetz, az IBM Security stratégiai és tervezési alelnöke a rendőrnyomozók munkáját segítő rendőrkutya példájával illusztrálta az MI szerepét a kibervédelemben. A hosszú évek alatt kiképzett rendőrkutyák képesek olyan nyomok felderítésére, amelyek elkerülhetik az őket irányító ember figyelmét. A folyamatosan tanuló MI eszközök ehhez hasonlóan alkalmazhatóak a fenyegetések kiszűrésében és megbízható tanácsadóként támogathatják a kiberbiztonsági szakembereket a megfelelő döntések meghozatalában.

IBM Watson: hatvanszor gyorsabban ismeri fel a veszélyt

A világon széleskörűen alkalmazott IBM Watson for Cyber Security megoldás – amit Magyarországon is egyre több ügyfél használ –, mesterséges intelligencia és kognitív tanulási képességei révén hatékonyan vethető be a kibertámadások elleni harcban. Watson „kiképzésének” alapját az IBM ún. X-Force Command Center adatbázisában a kibertámadásokról az elmúlt húsz év alatt összegyűjtött dokumentáció – több mint 800 terrabájt adat és 1 milliónál több szöveges dokumentum – adja. Ennek a hatalmas tudásanyagnak az elemezésével és felhasználásával a mesterséges intelligenciát használó védelmi rendszer a hagyományos biztonsági rendszereknél akár hatvanszor gyorsabban felismerheti a veszélyt. „A rendszer olyan mintákat is képes észlelni, amelyek egy még ismeretlen típusú, lehetséges támadás kibontakozásának első fázisaira utalnak. Watson tanácsot ad a fenyegetés kivédéséhez, és segít a válaszadás automatizálásában is. A mesterséges intelligenciára épülő kognitív kiberbiztonsági rendszerek gyorsasága és nagyfokú önállósága különösen nagy előnyt jelent a nagymértékű szakember hiány miatt várhatóan kialakuló krízishelyzetben. Az MI-t használó kibervédelmi rendszerek sohasem helyettesíthetik teljes egészében az IT szakembereket, de főszerepet vállalhatnak az emberi munka hatékonyabbá tételében.” – tette hozzá Rehus Péter.