Pedig korábban láttak a robotikában lehetőséget. 2017-ben még egy nyílt forráskódú, robotikai szimulációs környezetet is létrehoztak. Úgy látszik azonban, hogy ezen a területen egyelőre az adathiány komoly akadálya annak, hogy ebből az irányból lehessen közelíteni az általános MI-hez. Az OpenAI alapítója a már idézett podcastban azt mondta, hogy jobban hisznek a megerősítő tanulásban (nem lekódolják a fejlődés irányát, hanem visszacsatolás révén tanul az algoritmus), és egyelőre úgy tűnik, abban sokkal jobb eredményeket is tudnak elérni.

Kicsit a miénk is, és videón még talán sokáig gyönyörködhetünk benne

Mint *Andrew Ng* MI-szakértő írja, a döntés mögötte az MI-alapú robotika általános problémája húzódik meg. Hozza is a példákat: a Honda már 2018-ban bezárta robotikai leányvállalatát, az Asimót, amit általános célú „humanoid" robotnak szánt, és energiáit inkább céleszközök (célrobotok) fejlesztésére fordítja. Szintén bezárt a bostoni székhelyű Rethink Robotics, amely a dán Universal Robotsszal emberekkel együttműködő robotokat, ún. cobotokat fejlesztett, csak míg a dán vállalat elsősorban gyártóipari nagyvállalatok igényeit igyekszik kielégíteni, a Rethink egy általánosabb célú és a kkv-kat kiszolgálni képes irányban gondolkodott. A fejlesztési költségek azonban annyira elszálltak, hogy végül a céget bezárták, szabadalmait értékesítették (pl. az Universal Robotsnak).

De ugyanilyen válságjelenség Andrew Ng szerint az is, hogy a látványos kutyaszerű és humanoid robotjairól ismert Boston Robotics már a sokadik tulajdonosánál tart. A Google 2013-tól négy évig küzdött vele, aztán jött a minden zaftos technológiai cégre lecsapó SoftBank, majd idén nyártól a Hyundai sétáltathatja a robotkutyákat. Azt azonban nem tudni, hogy hosszabb távon megmarad-e a jelenlegi fejlesztési irány, vagy a Hyundai felhasználja a Boston Dynamics eredményeit az ipari robotjaihoz.

Azok a falánk algoritmusok!

Adrew Ng szerint ezek a történetek az MI-algoritmusok elképesztő adatéhségére hívják fel a figyelmet. Az pedig, hogy még egy robotflotta sem képes elegendő adatot termelni a fejlesztésekhez, rámutat, milyen távol vagyunk az általános MI-től. Mint Ng írja, egy csecsemőnek csupán egy testnyi adat elegendő ahhoz, hogy tanuljon.

Válogatta: Fonyó Istvánné
Forrás: https://bitport.hu

Biztonságos hibrid munkahelyeket akar? Vegyen fel minél több női alkalmazottat!

A férfi alkalmazottak sokkal több kockázatos tevékenységet folytatnak a neten, mint a nők. És ezen a házirendek nem segítenek.

Érdekes problémára hívja fel a figyelmet egy kutatás: egyértelműen összefüggés van az alkalmazottak biztonságtudatossága és neme között. És hogy miért érdekes ez? Mert a pandémia hatására egyre több vállalat tervezi a hibrid, azaz az otthoni és az irodai munkavégzést vegyítő munkakörnyezet állandósítását, ami felértékeli a biztonságtudatosság szerepét az IT-biztonságban, írja a kutatásról készített összefoglalójában a SecurityWeek. (Júniusban a Bitporton cikksorozatot szenteltünk a témának.)

Az IT-biztonságért felelős csapatoknak ki kell terjeszteniük a védelmet az akár ellenséges környezetben működő távoli személyi eszközökre is. Erre vannak kiváló termékek, és persze ott van a cégekre szabott házirend is. Ám nincs az az erős védvonal, amit a leleményes felhasználók akar-

va-akaratlanul ne tudnának kicselezni. Egy fiatal amerikai startup, a biztonságtudatossági képzésekre szakosodott SecurityAdvisor készített egy felmérést (PDF), amiben az alkalmazottak hibrid környezetben jellemző viselkedését térképezte fel.

Több mint húsz országra kiterjedően elemezték azokat a rosszindulatú e-maileket, veszélyes szoftvereket és webhelyeket, melyekkel az alkalmazottak (a kezdőktől a C szintű vezetőkig) kapcsolatba kerültek. Ez alapján öt magas kockázatú tevékenységet azonosítottak: a sikertelen hitelesítést; az adathalász emailekre kattintást; adware-ek és kémprogramok telepítését; a P2P szoftverek és saját VPN-ek használatát; végül, de nem utolsósorban a kalóz tartalmak streamingjét.

Sikertelen azonosítás mint kockázat?!

Mindezek közül talán a multifaktoros hitelesítés (MFA – Multi Factor Authentication) listára kerülése a legérdekesebb. Elvileg ugyanis ez csak azt bizonyítaná, hogy a hozzáférés-szabályozás jól működik. Csakhogy ez nem teljesen igaz, hiszen olyan esetekben hiúsul meg a hozzáférés, amikor az adott személynek van jogosultsága az adott vállalati erőforrások használatára. Ha ebben a rendszer nem következetes, az fölöslegesen terheli le a biztonsági csapatot, ráadásul megnehezíti az emberi hiba és a valóban rosszindulatú tevékenység megkülönböztetését. A kutatás szerint az otthonról dolgozók fele havonta legalább egyszer elhasal az MFA-n.

Konkrétabb fenyegetést jelentenek az adathalász levelek. A vállalati spamszűrők jellemzően ezek 1 százalékát nem ismerik fel, így száz spamből legalább egy el is jut az alkalmazott postafiókjába. Ez a vizsgált körben alkalmazottanként átlagosan havi öt levelet jelent, melynek 8 százalékára kattintanak is. Ez már egy néhány száz fős szervezet esetében is elég komoly kockázati tényező lehet.

Az alkalmazottak 3–4 százaléka telepít a gépére nem megbízható forrásból szoftvereket. Ezek a szoftverek általában a hivatalos úton beszerzett programoknál nagyobb valószínűséggel tartalmaznak veszélyes kódot (adware, kémprogram stb.). Az alkalmazottak mintegy 5 százaléka telepít peer-to-peer alkalmazásokat (pl. BitTorrent) és valamilyen saját beszerzésű VPN-t, hogy hozzáférjen földrajzilag korlátozott elérésű médiatartalmakhoz. A Security Advisor szerint ez utóbbi alkalmazások 38 százaléka rosszindulatú kódot tartalmaz, ráadásul az ilyen programok 82 százaléka hozzáférhet a felhasználó adataihoz.

Az alkalmazottak egy százaléka előszeretettel néz kalóz médiatartalmakat is (Putlocker, VidCloud stb.), ahonnan szintén könnyű begyűjteni gyanús-veszélyes kódokat.

Felső vezetők, férfiak, nők…

Az elemzés szerint a felső vezetők általában inkább ki vannak téve a célzott kibertámadásoknak, mint az átlagos alkalmazottak: például kb. ötvenszer gyakrabban szenvednek el adathalász jellegű támadásokat.

Ami pedig a fentebb felsorolt kockázatos tevékenységeket illeti, abban főleg a férfiak jeleskednek: a szándékos vagy figyelmetlenségből elkövetett kockázatos tevékenységeknek kevesebb mint a negyede (24 százalék) köthető a női alkalmazottakhoz. Ezt csak részben magyarázza a mintában a férfiak magasabb aránya (a teljes mintában 58 százaléka volt férfiak aránya). A női alkalmazottak jellemzően szabálykövetőbbek és kockázatkerülőbbek, mint a férfiak. Ez azonban nem valamiféle genetikai kód következménye, hanem tanulás eredménye. Azaz a férfiak is elsajátíthatják a biztonságtudatosabb viselkedést.

Válogatta: Fonyó Istvánné
Forrás: https://bitport.hu