

# Az IoT az alapokkal kezdődik

Számos, egymást kiegészítő technológia fejlődésének köszönhetően az Internet of Things (IoT) egyre gyorsuló növekedési pályán halad. Az 5G megjelenése zökkenőmentesebb végfelhasználói élményt biztosít a nagyobb számú összekapcsolt eszköz számára, a blockchain megkönnyíti az IoT-eszközök nyomon követését, a mesterséges intelligencia és a gépi tanulás pedig könnyebben hozzáférhetővé és alkalmazhatóvá vált, ami az eszközfunkciók szélesebb körét teszi lehetővé az összekapcsolt ökoszisztémában.

Az IoT felhasználási eseteinek széles skálája ismert, a pénzügyi szolgáltatásoktól kezdve az egészségügyön át a kiskereskedelemig. A piaci szereplők felismerték, hogy alapvető fontosságú a jól összekapcsolt digitális vállalkozások létrehozásához: az IDC előrejelzése szerint az IoT-re fordított globális kiadások 2023-ban elérik az 1,1 billió dollárt, ami 52%-os növekedést jelent a 2019-es kiadásokhoz képest.

"A csatlakoztatott eszközök pusztán mennyisége miatt a hálózatok sebezhetőek a hackerekkel szemben, akik a lánc egyetlen láncszemén keresztül szereznek hozzáférést. Az adatlopás hatékony ellenintézkedések nélkül kockázatot jelent. Egyes ágazatok a többenél nagyobb kockázatnak vannak kitéve – például a pénzügyi szolgáltatások és az egészségügy területén a védett személyes adatokat, illetve a személyes egészségügyi adatokat gyakran keresik eladásra a sötét weben. Azoknak, akik vezető szerepet akarnak betölteni a bomlasztó technológiák bevezetésében, az adatbiztonság garantálása kritikus elem" – mondta Szász Beáta, a Deloitte technológiai tanácsadás üzletágának senior tanácsadója.

A Deloitte felméréséből kiderült: a biztonsági tesztelés (57%) volt a válaszadók által említett legnagyobb kihívást jelentő szempont az IoT-alkalmazások tesztelésében - az adatbiztonság hitelesítése az üzembe helyezés előtt valóban kritikus fontosságú, és rendkívül összetett lehet. Az ezt követő kihívások kiegyensúlyozott eloszlást mutatnak: az infrastruktúra szükségessége (45%), a szükséges IoT-eszközök (44%) és a tesztautomatizálási stratégia (41%) szorosan követik egymást. Az összekapcsolt rendszerek megértéséhez és a validálások elvégzéséhez szükséges megfelelő erőforrás-képzettségek szükségessége (33%) szintén fontos volt.

A kihívások megfelelő kezelése összetett feladat. Több időt és erőforrást kell fordítani az IoT-alkalmazások biztonságának tesztelésére, és az összekapcsolt rendszerek kiépítéséhez és teszteléséhez szükséges megfelelő infrastruktúra kialakítására, különös figyelemmel a felhasználók megnövekedett mobilitási igényeire, a hálózat rendelkezésre állására és sávszélességére, valamint a hatalmas adatmennyiségek kezeléséhez szükséges adatközponti kapacitásokra. A tesztelési stratégia prioritizálásakor az IoT legnagyobb függőségeit – minimális késleltetés és gyors adatmozgás – kell szem előtt tartani. Az olyan változókat, mint az eszközök képessége, a Wi-Fi beállítása és a hálózati infrastruktúra, előzetesen alaposan validálni kell.

## Hogy érdemes elkezdni az IoT-tesztelést?

A szélesebb körű tesztelési stratégia alapos meghatározása kritikus fontosságú, és bár a feladat nagynak és összetettnek tűnhet, néha a leghasznosabb visszatérni az alapokhoz. A „zajon való átlátáshoz” felhasználó-központú megközelítést érdemes alkalmazni: azonosítani kell azon eszközök kombinációját, amelyek egy meghatározott időintervallumon keresztül folyamatos felhasználói forgalmat bonyolítanak, vagy amelyekben a forgalom hullámzik. A legsebezhetőbb, vagy a potenciális

megbízhatósági, skálázhatósági és rendelkezésre állási problémák szempontjából kell meghatározni a tesztelendő alkalmazásokat. Ez a megközelítés támogatja a támadásoknak leginkább kitett alkalmazások folyamatos tesztelését és validálását. A házon belüli diagnosztikai megoldások és IoT-laborok végzik el legjobban a csatlakoztatott ökoszisztéma validálását, a telepített emulátorok különböző eszközöket és szoftveralkalmazásokat imitálnak, hogy értékelni lehessen az olyan problémákból eredő potenciális hibákat, mint a szoftverfrissítések, hardverfrissítések, hibalehetőségek és hálózati problémák. Végül, fel kell mérni az eszközök és szoftveralkalmazások skálázhatóságát az adatáramlás jelentős késleltetés nélküli fenntartása érdekében. Fontos, hogy az alkalmazásoknak frissítés közben is rendelkezésre kell állnia, hogy az adatok folyamatos áramlása mindenkor biztosított legyen.

"Az 5G az IoT-elfogadás gyors terjedését eredményezte, számtalan olyan felhasználási esetet nyitva meg az iparágakban, amelyek mélyebb élményeket teremtenek a végfelhasználók számára. A sebezhetőségek és a biztonsági kihívások azonban megsokszorozódnak egy ilyen hatalmas és összekapcsolt ökoszisztémában. A komplexitással kapcsolatos kihívások kezelése érdekében előre meg kell határozni egy átfogó IoT-tesztelési stratégiát, amely az alapokhoz – az eszközök prioritásainak felhasználó-központú megközelítésekkel történő meghatározása, széles körű mintavétel, házon belüli laboratóriumok és emulátorok, valamint alapos skálázhatósági értékelések – nyúlik vissza" – foglalta össze Bakó Béla, a Deloitte Magyarország Technológiai tanácsadás üzletágának menedzsere.

Sajtókapcsolat:

- Bakó Béla, menedzser
- bebako@deloittece.com

Eredeti tartalom: Deloitte Magyarország

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:

<https://hellosajto.hu/6621/az-iot-az-alapokkal-kezdodik/>