ENTERPRISE OF THINGS

Egy konzol mind felett

A hálózatba kapcsolt szenzorok, eszközök és egyéb műszerek, vagyis az IoT-eszközök az otthonoktól az ipari létesítményekig mindenütt számtalan új lehetőséget nyitottak meg az adatgyűjtésre és beavatkozásra. Az új lehetőségeknek azonban árnyoldalai is vannak, amelyek közül kiemelkedik a biztonság kérdése.

CSINOS TAMÁS, CLICO

FORRÁS: ITBUSINESS

ALMÁSI ZSOLT, CLICO

FORRÁS: ITBUSINESS

Az IoT-eszközök hírhedtek arról, hogy mennyire nem biztonságosak, ami már nemcsak informatikai biztonsági problémákat vet fel, de konkrétan fizikai katasztrófához is vezethet, ha mondjuk egy gyár vagy közmű vezérlőrendszere felett veszik át az irányítást a hackerek.

Az IoT-eszközök alapvetően azért nem biztonságosak, mert nem klasszikus számítógépnek készültek – mondta egy korábbi ITBUSINESS Club rendezvényen *Csinos Tamás,* a Clico Magyarország country managere. Tervezésük során a teljesítményüket és a funkcionalitásukat alárendelték annak, hogy minél kisebb energiafelhasználással és minél hosszabb ideig működjenek. Emiatt a legtöbbször nem implementálnak bennük erős biztonsági funkciókat. *(Lásd a „Hatékony, de nem biztonságos” című keretet!)*

Érdekes módon a fogyasztói felhasználásra szánt eszközök általában biztonságosabbak, mint az ipari-üzleti felhasználásúak. Ennek oka, magyarázta Csinos Tamás, hogy a consumer berendezések sok funkciósak, és rendszerint viszonylag hosszú a fejlesztési ciklusuk, így van idő a biztonsági funkciók kifejlesztésére és beépítésére. Ezzel szemben az ipari rendszereknek többnyire csak egyetlen funkciót, de azt kiemelkedő megbízhatósággal kell ellátniuk. Ezért a működési vagy üzembiztonság mindig is elsőbbséget élvez az informatikai biztonsággal szemben.

A kulcs a kontrollált hozzáférés

Különösen sok gondot tud okozni, ha az IoT- (vagy éppen OT-, operations technology) eszközöket össze kell kapcsolni a meglévő informatikai hálózatokkal. Az IT-rendszereket és -hálózatokat többnyire már ellátták védelmi funkciókkal, elérve egy adott biztonsági szintet. Ezt a szintet súlyosan veszélyezteti, ha ellenőrzés nélkül beengedik az IoT-eszközök felől jövő forgalmat.

„Csak úgy tudjuk megvédeni informatikai rendszereinket az eszközökben rejlő sérülékenységektől, ha az első pillanattól kezdve kézben tartjuk a hálózathoz való hozzáférést”, foglalta

össze a teendőket Csinos Tamás. Ennek több lépése van, és egyiket sem szabad elhanyagolni.
Először is, minden pillanatban tisztában kell lenni azzal, hogy milyen eszközök csatlakoznak a hálózathoz. Azt hihetnénk, hogy ez alapkövetelmény, de még az IT-biztonságra amúgy odafigyelő cégek sem feltétlenül rendelkeznek naprakész listával.
A dolgozók igen találékonyak, és a szakemberek már találkoztak engedély nélkül telepített wifi-hozzáférési ponttal (hogy a kolléga a magántelefonjával is hozzáférjen a céges wifihez) vagy éppen Raspberry Pi mikroszámítógéppel. „A hálózat folyamatos monitorozása kulcskérdés, mert akár percek alatt ki lehet lopni a vállalati adatvagyont", figyelmeztetett Csinos Tamás.

Csak semmi bizalom!

A második lépésben a hálózaton felderített eszközökre funkció szerinti csoportosításban szabályokat kell hozni. Más besorolás alá esik egy nyomtató, mint a pénzügyi igazgató számítógépe vagy mondjuk egy biztonsági kamera. Ha az informatikusok azonosítottak egy különösen sebezhető, de nélkülözhetetlen eszközt, annak védelmére speciális szabályokat vezethetnek be. Szintén speciális szabályokat kell alkotni az IoT-eszközökre, például egy irodaház épületmenedzsment rendszerét alkotó vezetékes és vezeték nélküli szenzorokra, vezérlőkre vagy a gyártósori PLC-kre.
A harmadik lépésben ezeket a szabályokat rá is kell erőltetni a nevezett eszközökre. Ha valamilyen szempontból nem felel meg a számára megalkotott szabályoknak – mondjuk, nem a legfrissebb szoftver fut rajta, vagy hiányzik valamilyen biztonsági elem –, addig nem, vagy csak korlátozottan férhet hozzá a hálózati erőforrásokhoz. A jó rendszer arra is képes, hogy külső biztonsági eszközöket (tűzfalakat, végpontvédelmi eszközöket) bevonjon a szabályrendszer érvényesítése érdekében.
„Manapság már nem működik a »trust, but verify« hozzáállás, vagyis hogy megbízunk az eszközökben, de ellenőrizzük azokat. Az új jelszó a »zero trust«, vagyis hogy csak azokat az eszközöket, szoftvereket, szolgáltatásokat engedjük be a hálózatunkba, amelyek esetében 100 százalékig meggyőződtünk, hogy úgy működnek, ahogy mi szeretnénk", tette hozzá Csinos Tamás.

Minden látható

A klubrendezvényen *Almási Zsolt,* a Clico rendszermérnöke be is mutatta a Forescout platformját, amely a fenti funkciókat

FORRÁS: ITBUSINESS

nemcsak a szokványos informatikai eszközök, hanem az IoT- és OT-eszközök esetében is ellátja.
Különlegessége, hogy más hálózat- és forgalommonitorozó eszközökkel ellentétben nem telepít kódot (agentet) a megfigyelni és ellenőrizni kívánt végpontokra. Ez egyrészt csökkenti a végpontok terhelését, másrészt gyártófüggetlen lehet, hiszen nem csak egy nagy gyártó hálózati berendezéseit tudja kezelni.
Számos rendszerhez már előre elkészített csatolókkal kapcsolható, így programozói tudás sem kell ahhoz, hogy a tűzfalakat, végpontvédelmi eszközöket integrálják hozzá. Integrálásra pedig szükség van, mert a Forescout, mint egy karmester, csak észlel, megfigyel és irányít, de a konkrét beavatkozásokat, a szabályok végrehajtását más eszközökre bízza.
Az agent nélküli működés teszi lehetővé azt is, hogy az ipari (OT-) rendszerek felügyeletét is ellássa. (Erre a képességre a korábban SilentDefense névre hallgató megoldás megvásárlásával tett szert a Forescout.) Az ipari rendszerek esetében ugyanis a működésbiztonság mindent felülíró követelmény, így agentet sem szabad telepíteni rájuk, és aktív hálózatszkenneléssel sem lehet beleavatkozni a kommunikációba.
A Forescout részét képező eyeInspect az IoT- és OT-eszközök esetében végzi a hálózatra csatlakoztatott eszközök feltérképezését; a hagyományos informatikai végpontoknál ugyanezt a feladatot az eyeSight modul látja el. Adatbázisaik révén pontos képpel rendelkeznek számtalan IT- és OT-eszköz sérülékenységeiről, a firmware-ekről, frissítési szintekről vagy éppen kommunikációs képességekről.
A külső rendszerekkel való kapcsolattartásra az eyeControl és az eyeExtend nevű modulok szolgálnak. Előbbi kész csatolókat tartalmaz a támogatott szoftverekhez, utóbbi pedig programozási interfészeket mindazokhoz az eszközökhöz, amelyeket még nem ismer a Forescout.
Legnagyobb előnyeként mégis azt emelte ki Csinos Tamás, hogy egyetlen eszközből, egyetlen konzolból kezelhetők mind az informatikai, mind az ipari és IoT-eszközök – ebből lesz az Enterprise of Things, vagyis minden, ami a vállalati hálózatra csatlakozik. ■

Hatékony, de nem biztonságos

Csinos Tamás felidézett egy hazai esetet, amikor egy okosmérő fejlesztésénél energiatakarékossági okokból viszonylag kis teljesítményű processzort használtak. Mint kiderült, a választott processzor olyan gyenge lett, hogy két mérési ciklus között nem tudta legenerálni a továbbítandó adat titkosításához szükséges, kellően erős aláírási kulcsot… Megoldásként azt találták ki, hogy rövidebb kulcsot alkalmaztak, ami persze nagymértékben csökkentette a biztonságot.