CSINOS TAMÁS ESSZÉJE

A felhő, meg az ő biztonsága

Tele van a szaksajtó a felhős szolgáltatásokat dicsőítő cikkekkel, a felhős cégek negyedéves győzelmi jelentéseivel (erről még később), burjánzanak azok a vélemények, amelyek összemossák a digitalizációt a felhős technológiákra való áttéréssel, az olcsón hozzáférhető, jó minőségű felhős IT-megoldások versenyelőnyt, felzárkózást (nem kívánt törlendő) bizonygató csábításokkal. Az is szóba kerül hébe-hóba, hogy bizony ezek biztonsági és adatvédelmi szempontból megosztott felelősségű rendszerek és szolgáltatások, de melyik az a lelkes döntéshozó, aki, amikor végre meglátja a digitális transzformáció nevű alagútban a fényt, azonnal elkezd kockázatokat számolni, és védelmi szabályzatokban és új típusú, megelőző és a bajt esetleg kezelni is képes rendszerekben gondolkozni?

CSINOS TAMÁS, CLICO

FORRÁS: CLICO

Van a felhasználóknak egy olyan csoportja, akiknek a felhő, mint ördögnek a szenteltvíz, hallani sem akar róla, mert az ő szabályozói környezete olyan, hogy tudja, hogy mit rántana magára egy audit esetén, vagy olyan, amely explicit megtiltja a publikus felhőkben kínált IaaS-, SaaS-, PaaS-dolgok használatát.
A kétféle megközelítésben talán van egy közös: körülbelül biztosra vehető, hogy egyrészt minden cégnél és szervezetnél már most is használnak valamilyen nem felhős rendszert. („Józsikám, dobd már át dropboxon-boxon-onedriveon-gdrive-on, akármilyendrive-on a szerződéstervet, tábláról nem látom a szerveren!”, ugye ismerős?) Valamint azt is feltételezhetjük, hogy valaki vagy valakik a cégen-szervezeten belül már ismerkednek – neadjisten a biztonságért felelős kollégák tudta nélkül, ó, jaj – minimum a privát felhőkben szokásos technológiák kiszolgálta alkalmazásokkal.

A sötét erdő

Sok oka lehet, hogy ez a helyzet előállt, néhányat megpróbálok megfejteni. Az egyik talán, hogy a kockázat-védekezés arány még egy közepes méretű cégnél is elérte azt a szintet, hogy a meglévő IT-infra mellé fel kellene építeni egy még egyszer akkora biztonsági infrát. Elég csak a naplógyűjtés és elemzés problémakörére gondolni, a rengeteg forrásrendszer rengeteg adatát gyűjteni, és értelmesen feldolgozni képes földi infrastruktúra gigászi helyen és számítási kapacitással kell, hogy rendelkezzen. Aztán, ahogy újabb és újabb védelmi rétegeket kezdünk el bevezetni, akár megelőző, akár valamilyen korábbi hibát korrigáló céllal, azoknak megint csak saját infra kell, és megint csak hatalmas étvággyal konzumálják a példa szerinti napló elemző kapacitásokat. Öngerjesztő folyamat, ha abban a szerencsés helyzetben vagyunk, hogy a szervezet megfelelő mértékben biztonságtudatos, ami jó, akkor kb. biztos, hogy abban a helyzetben is vagyunk, hogy képtelen lépést tartani a megjelenő fenyegetésekre adott adekvát válaszok iránti igénnyel, sem financiálisan, sem emberi erőforrásokkal.
Innen egyenes az út a nyúl gödrébe: jöjjön az AI, az ML és bármi, ami enyhítheti ezt a viszkető érzést.
A másik, és talán nem közösít ki a szakma, ha leírom, hogy a biztonsági rendszereket és megoldásokat fejlesztő mégoly neves nemzetközi játékosok (és forgalmazóik is) hiú ábrándba kergették az ügyfeleket. A legújabb, minden-ellen-is-jó sárkányfüvek a szirének csábításával megspékelve olyan védelmi szinteket lebegtettek meg, amelyekhez olyan szintre gyúrt üzemeltetői, biztonságirányítási gárdára lenne szükség, amilyet itthon talán, ha pár tucat szervezet engedhetne meg magának.
És itt ketté is bontanám a megfejtést a titkon, akár búvópatakként, akár tudatosan feltörő felhős irányok kontrollálása és védelme részre, illetve bizonyos, most még inkább földi infrastruktúrákban használt biztonsági alrendszerek felhőbe költöztetésével kapcsolatos részre.

Alkalmazásfejlesztés betépve

Talán az IT legdinamikusabban fejlődő ága az alkalmazásfejlesztés. Az olcsó sávszélesség, az okoseszközök számítási kapacitásának ugrásszerű fejlődési lépcsői a „webes” technológiák egyeduralkodását hozták. És mindezt ami ezzel jár, a napi akár több száz alkalmazás-mikroverziót, buildet, a felfokozott tempójú, agilis módszertanokkal való fejlesztést, a pörgést, a feszített ütemet.
A megrendelők felhasználók el vannak kényeztetve, egy robusztus alapfunkciókkal induló megoldás akár hetente kap új feature-t, szebb felületet, gyorsabb működést. És ebbe a gyönyörűen kidolgozott folyamatba akar beleavászkodni a biztonság. Aki nyilván képtelen napi 500 builden kódellenőrzést végezni, véleményezni, szabályzatokkal adatbázisokat, struktúrákat, titkosítási szinteket és algoritmushasználatokat összevetni – egyszóval, mindent csinálna, ami lassítja a munkát. Az alkalmazásgazdáknak a legtöbb esetben púp a hátukra az egész.
Szükség van egy (illetve, hát nyilván sok…) megoldásra, amelyek lehetővé teszik, hogy a biztonság, mint olyan, egy felfelé emelkedő spirálban épülhessen be a kódba, a háttérrendszerekbe, a konténerekbe, magába az alkalmazásba. Szóval, szükség van valamire, amely anélkül ad segítséget a fejlesztőknek, hogy akadályozná őket, anélkül ad támpontot a biztonságirányításnak, hogy örök harag legyen a két csapat között. Szerencsére erre is van ötletünk, több is.

És akkor a biztonságról

A másik problémakör a biztonsági alrendszerek felhőbe – SaaS-modellel, azaz komplett megoldás igénybevétele – szóval, a felhőbe „költözése”. Első példaként említeném az email-ekkel kapcsolatos problémát, ami ahhoz képest, hogy a sikeres támadások 96-97 százalékában szerepet játszik az email, mint a támadás szállítóeszköze, origója, sine qua non-ja, még mindig a kívánatosabbnál elhanyagoltabb terület. Azért, mert macerás üzemeltetni. Kell hozzá szerver, finomhangolni kell a szabályrendszert, kezelni a karantént, „szupportálni a júzert”, ugye. És akkor jön a gigacég, és minden nyűgöt levesz a vállunkról a felhős levelezőrendszerrel.
Hát, sajna nem. Valóban emel a biztonsági szinten az O365-M365 levelezés használata, de korántsem ad az erre szakosodott megoldásokat még csak megközelíteni képes biztonságot. Ezekből adja magát, hogy célszerű a levelezéssel kapcsolatos biztonsági kérdéseket felhős megoldással kezelni, hiszen a levelek kintről jönnek, ha kint szűrjük őket, akkor egyáltalán nem juthat be a céges infrára veszélyes email, vagy nem juthat el még home office-ban dolgozó kolléga gépére sem. Mégis, amikor a felhős email-szűrésről beszélünk, a legtöbb cég ódzkodik még meghallgatni is.
Második példaként hoznám webes tartalmak biztonságát, aminek rögtön két ága is van, ez egyik de facto felhős: a különböző engedélyezett vagy „árnyék-IT” által használt, más SaaS-típusú erőforrások elérését szabályozni képes biztonsági brókerek (cloud access security broker, CASB), illetve a kvázi hagyományosnak tekinthető webszűrő- (manapság inkább komplex webbiztonsági-, mint csak szűrő-) megoldások. Fogalmazzunk úgy, hogy a CASB a felhős üzleti alkalmazások védelemére való, a web security pedig a publikus internet biztonságos használatát teszi lehetővé.
Ezeknél is, mint az email-szűrőknél, a felhős megoldásoktól való tartózkodás nem igazán érthető, hiszen minden olyan, amit vagy amitől védeni akarunk, az a „felhőben”, kint a hidegben van, azaz a védelmet sincs sok okunk lehozni a földi infrára. Főleg, hogy mind az email, mind web biztonsági megoldások a szükséges intelligencia frissítéseket, lenyomatokat, ellenőrzéseket a gyártó felhőjéből kapja, egyébként képtelenek lennénk a „hidegben” történő változásokat lekezelni.
(A szerző a Palo Alto Networks és a Forcepoint magyarországi nagykereskedője) ■