Írta: Oracle
2019. március 27. szerda, 14:11

Egyre több vállalat helyezi a felhőbe az üzemkritikus működési folyamatait és a legbizalmasabb adatállományait, azonban a felhő alapú megoldásokhoz kapcsolódó biztonsági kihívások továbbra is jelentősek – derül ki az Oracle and KPMG Cloud Threat Report 2019 jelentéséből. Az immár második éve végzett felmérésben a válaszadók 72 százaléka állította, hogy a nyilvános felhő biztonságosabb, mint a saját céges adatközpontjuk, ezért inkább a felhőbe helyezik adataikat. Az átláthatóság hiánya azonban megnehezíti a cégek számára annak megértését, hol és hogyan kezelik bizalmas adataikat a felhőben.

Az Oracle és a KPMG közös felmérése szerint 2018 és 2020 között 3,5-szeresére növekszik azon vállalatok száma, amelyek adataik legalább felét a felhőben tárolják, emellett a vállalatok 71 százaléka azt állította, hogy a felhőben tárolt adatok többsége bizalmas információ, szemben a tavaly mért 50 százalékkal. Ugyanakkor a felmérésben résztvevők többsége (92 százalék) aggódik, hogy a munkavállalóik betartják-e az adatok védelmét szolgáló felhőbiztonsági szabályozásokat.

A jelentésből az is kiderül, hogy a felhőszolgáltatások üzemkritikus jellege miatt a felhőbiztonság mára stratégiai szempontból is elengedhetetlenné vált. A felhőszolgáltatások napjainkban nem harmadrangú IT kiegészítőként vannak jelen a vállalati működésben, hanem számos üzleti érdeket érintő, alapvető jelentőségű funkciót szolgálnak ki. Az Oracle és a KPMG idei felmérése több kulcsfontosságú területet tárt fel, ahol a vállalatok számára kihívást jelent a felhőben tárolt adatok védelme.

- A megosztott felelősség körüli bizonytalanságok kibervédelmi incidenseket eredményeztek. A felhőmegoldásokat használók 82 százaléka tapasztalt biztonsági incidenseket, amelyek a megosztott felelősségi körök értelmezésének hibáiból adódtak. Míg a válaszadók 91 százaléka rendelkezik pontos belső szabályozással a felhő alkalmazásának tekintetében, 71 százalékuk biztos benne, hogy a munkavállalók megsértik a szabályokat, ami kibertámadásokhoz és adatvédelmi incidensekhez vezet.
- Az információbiztonságért felelős vezetők (Chief Information Officer – CISO) túl sokszor szorulnak a partvonalra. A CISO-k 90 százaléka mondta, hogy nincs tisztában a szerepkörével az SaaS (Software as a Service) alkalmazások védelmével kapcsolatban, ellentétben a felhőszolgáltatói környezettel. A CISO-k 90%-a úgy nyilatkozott, hogy SaaS (Software as a Service) szolgáltatás védelmével kapcsolatban nincs tisztában a szerepkörök megosztásával a saját, illetve a felhőszolgáltató környezete között.
- Továbbra is az átláthatóság a legfőbb biztonsági probléma. A válaszadók 38 százaléka számára a legnagyobb kihívást a kiberbiztonsági incidensek észlelése és azok kezelése jelenti

a felhőben. A felmérésben részvevők 30 százaléka szerint biztonsági kihívást jelent számukra, hogy a meglévő hálózati biztonsági eszközeikkel nem tudják a felhőben lévő szerveren futó alkalmazásaikat monitorozni.

- A felhőalkalmazások illetéktelen használata és a biztonsági ellenőrzések hiánya veszélyezteti az adatokat. A válaszadók 93 százaléka mondta, hogy még mindig problémát okoz számukra a „shadow IT”, ahol a munkavállalók engedély nélkül használják saját eszközeiket, tárhelyeiket vagy fájlmegosztó szoftvereket a vállalati adatok kezelésére. A vállalatok mintegy fele említette a csalások és az adatok sérülékenységének gyakori okaként a biztonsági ellenőrzések hiányát és a helytelen konfigurációkat. Emellett a vállalatok 26 százaléka számára a legnagyobb kiberbiztonsági kihívást a felhőszolgáltatások jogosulatlan használata jelenti.

“Az Oracle-KPMG jelentés megállapításai a közép-európai vezetők számára jövőbe tekintési lehetőséget nyújtanak, amit érdemes hasznosítani. Valamennyi késéssel Magyarországon is ugyanezek a felhőhasználati trendek és a velük járó problémák lesznek jellemzők. Vegyük úgy, hogy nekünk több időnk van informáltan felkészülni arra az időre, amikor a magyar vállalatok és akár az államigazgatás is tömegével futtatnak majd üzletkritikus alkalmazásokat nyilvános felhőben.

A jelentésben megkérdezettek körében a legfontosabb munkafolyamatok már a felhőben futnak, ezért vállalataiknak az eddiginél sokkal jobban koordinált, integrált és többrétegű biztonsági stratégiára van szüksége. Ezen stratégiáknak része kell legyen a dolgozók biztonsági képzése és tevékenységük monitorozása ugyanúgy, mint mesterséges intelligencia használata.

Adatvédelmi, audit és törvényi megfelelési szempontból is sokat levesz a személyzet válláról egy ilyen modern stratégia. Ugyanakkor nemcsak új biztonsági megoldásokra és modellekre van szükség, hanem azoknak a gyakorlatba való hatékony átültetésére is. Fontos, hogy a felhasználók átlássák, mit szolgálnak a biztonsági szabályozások és azokat be is tartsák, illetve betartassák velük.” – mondta Szuhai Gusztáv, az Oracle biztonsági megoldásokért felelős kereskedelmi vezetője.

“Magyarországon tapasztalt érdekesség, hogy bár a kulcs-rendszerek felhőbe telepítése még nem olyan elterjedt, az említett gépi tanulás alapú, felhőben futó korszerű menedzsment megoldásokat sokan szívesen alkalmaznák a saját, hagyományos adatközpontjaik monitorozására – és erre adott is a lehetőség. Az Oracle által fejlesztett üzemeltetési és biztonsági menedzsment megoldások egyaránt használhatók hagyományos vagy felhős környezetben, illetve ezek tetszőleges kombinációjában, és az eddig alkalmazott monitorozó eszközöktől eltérően, az infrastruktúra minden rétegét egyben, egy felületen kezelhetően, holisztikusan monitorozzák” – tette hozzá Szuhai Gusztáv.

A jelentés főbb megállapításai:

- Az automatizálás segíthet a tartósan fennálló patchelési problémákban: a megkérdezettek 51 százaléka állította, hogy a patchelés hátráltatta az IT projekteket, a vállalatok 89 százaléka pedig automatikus patchelési stratégia bevezetését tervezi.
- A gépi tanulás csökkentheti a fenyegetettségek számát: a válaszadók 53 százaléka használ gépi tanulást a kiberfenyegetések ellen, 48 százalék pedig többfaktoros azonosítást (Multi-factor Authentication – MFA) alkalmaz, amelynek segítségével automatikusan beiktathatnak egy második hitelesítési faktort a szokásostól eltérő felhasználói viselkedés észlelése esetén.
- Kockázatok az ellátási láncban: az üzemkritikus szolgáltatásokat el kell szigetelni, mivel az ellátási lánc veszélyeknek való kitettsége az esetek 49 százalékában vírusok bejutásához vezetett, amelyet az esetek közel felében (46%) illetéktelen adathozzáférések követtek.

- A megosztott felelősségi körökkel kapcsolatos bizonytalanság növekedése egyre több biztonsági incidenshez vezet: tízből egy vállalat képes elemezni a biztonsági eseményekhez kapcsolódó adatok legalább 75 százalékát, és a felhő felhasználóinak 82 százaléka került már biztonsági incidensbe a megosztott felelősségi körökön alapuló felhőbiztonsági modellek körüli bizonytalanság miatt.
- A felhő növekvő alkalmazása kiterjesztette a core-to-edge modellt: az egyre mobilisabb munkaerő, amely mind a telephelyi, mind a felhőben elérhető alkalmazásokhoz is képes hozzáférni, drasztikusan megnehezíti a kiberbiztonsági szakemberek munkáját a kockázatok és fenyegetettségek tekintetében. 2018-ban még a képzésekbe fektettek a legtöbbet, idén viszont már a tréningek a második helyre szorultak, és a végponti védelem vette át a vezető szerepet (pl. WAF, CASB, Botnet/DDoS Mitigation ellenőrzések).