FORTINET

Felhő? Biztonságosan? Így lehet!

A felhőtechnológia korszakában az adatok feldolgozása közmű jellegű szolgáltatássá változott, középpontjába a megosztott infrastruktúrát helyeztük. Az új működési modellben, ahol a hálózat, adattárolás, szerverek és még az adatközpontok is megosztott erőforrásokká válnak, fontos megérteni a nyilvános, privát és hibrid felhő biztonságával kapcsolatos kockázatokat.

FORRÁS: FORTINET

Egyre több vállalat bízza a felhőre IT-infrastruktúráját: az IDG 2020-as „Cloud Computing” tanulmánya szerint a cégek 81 százaléka legalább egy alkalmazását felhőben működteti. A fenyegetések az új működési környezethez alkalmazkodnak, nemcsak bonyolultabbak és kifinomultabbak, hanem az új hálózati elemeket is célba veszik, ahol az IT-biztonság még gyermekcipőben jár.

A nyilvános felhő biztonsága

A szervezetek főként biztonsági okokból tartottak a nyilvános felhő szolgáltatások igénybevételétől. A megosztott felelősség modell szerint a felhőszolgáltató egy adott szintig felelős a biztonságért, de a vállalatoknak is van feladatuk. A szolgáltató arra összpontosít, hogy biztonságos felhőinfrastruktúrát teremtsen, megfelelően elszigetelje egymástól a bérlőket, óvja a számítási kapacitást, az adattárolást és a hálózatot. Megteremti ügyfeleinek a hatékony biztonság terét.
A cégeknek egy olyan rugalmas biztonsági megoldást kell választaniuk, amely hatékony védelmet biztosít a működési környezet számára, miközben a teljesítményt, méretezhetőséget és a multicloud együttműködést nem gátolja. A központosított menedzsment, a nyílt API-integráció, az automatizáció és a felhőplatform-megközelítés a multicloud környezetek szolgáltatói integrációját segíti elő.

A privát felhő biztonsága

A privát felhő biztonsági megoldásainak alapból támogatniuk kell a szoftver központú megközelítést. A software defined networking (SDN) fejlődése azt jelenti, hogy a hálózati erőforrások nem egy dedikált fizikai hardveren találhatók. Adatközpontokban belső szolgáltatásként működnek, rengeteg fizikai vagy virtuális eszközt, helyszínt lefedve. Emiatt nem elég a hardvert megvédeni, a biztonságot ki kell terjeszteni a valós idejű üzleti követelmények szerint, dinamikusan konfigurált szolgáltatásokra.
A Fortinet szoftver alapú biztonsági megoldásait a vezető SDN, virtualizációs és hálózati virtualizációs platformok tanúsították, kiválóan használhatjuk bármely privát vagy hibrid felhő környezetben.

A hibrid felhő biztonsága

A felhőben az üzleti szempontból kritikus alkalmazások és adatok szegmentációjával csökkentjük a rendszerek kitettségét. Hibrid környezetben az adat, munkafolyamatok és alkalmazások a külső és belső helyszínek, a harmadik fél által biztosított, és belső hálózatokhoz csatlakoztatott szolgáltatások között mozognak. Egy hibrid felhő biztonsági megoldásának megfelelő védelmet kell biztosítania az összes bizalmas kapcsolódási pont számára a hálózati kapcsolódás egyéni kockázati profilja szerint.
A hibrid felhőkörnyezetek jelentik a legnagyobb kihívást a biztonsági megoldás szempontjából. A privát és publikus felhőben szétszórt eszközök láthatósága kritikus, hiszen a biztonsági csapatok csak egy központi menedzsmentmegoldás segítségével kezelhetik a teljes rendszert.

A Fortinet Security Fabric garantálja a konzisztens biztonságot és vizibilitást a teljes digitális támadási felületen, legyen az on-premise vagy többféle felhőt átfogó. *(X)*