Offline: Computerworld Magazin, 2019. április 24. – 22. oldal

KELENHEGYI PÉTER

Időtényező

Kiberkalózok a mézben

Egy év alatt két és félszeresére nőtt a kiberbiztonsági incidensek száma, állítja egy friss kutatás, hozzátéve: az érintettek nem állnak készen gyors elhárításukra.

Tavaly a veszélyes incidensek száma másodpercenként 3,8 millió volt, míg egy évvel korábban „csupán" 1,4 millió. Az elemzés szerint átlagosan 4 óra 37 perc volt az úgynevezett kitörési idő, azaz a behatolás után körülbelül ennyi időbe telt, amíg a támadók megkezdték mozgásukat a feltört szervezeten belül. A Micro Focus éves jelentésében *(State of Security Operations)* 144 biztonsági műveleti központ (Security Operations Center, SOC) működését vizsgálták összesen 33 országban, egyúttal értékelték, azok mennyire érett és fejlett kiberbiztonsági képességekkel rendelkeznek.

SOC-ásos szinten

Nos, a központok érettsége 7 százalékkal nőtt az előző évhez képest, ugyanakkor 20 százalékuk még az első érettségi szintet sem éri el, ami azt jelenti, hogy eleget tesznek ugyan a biztonsági események monitorozásához szükséges minimális követelményeknek, de nem készítenek semmilyen dokumentációt, és tevékenységeik is ötletszerűek.

Mindössze a vizsgált központok 5 százaléka működik az ajánlott szinten. Ezeken a helyeken pontosan meghatározzák, milyen műveletekre van szükség a biztonság fenntartásához, és tevékenységeiket azok alapján végzik. A folyamatok azonban rugalmasak és proaktív módon változtathatók, így a hatékonyság optimalizálható. Szükség esetén tehát gyorsan tudnak reagálni az eseményekre, mivel nem fordítanak felesleges időt a túlszabályozott környezetek felügyeletére és működtetésére.

A megfelelő védelemhez átfogó biztonsági stratégiára van szükség, amely kiterjed az adatok, az alkalmazások, az eszközök és a személyazonosságok védelmére, illetve a biztonsági események kezelésére, ezeknek pedig összhangban kell állniuk egymással, tanácsolják a Micro Focus szakértői. Érdemes például integrálni a személyazonosságokat kezelő és irányító rendszereket a biztonságiinformáció- és eseménykezelő (SIEM-) megoldással, így ugyanis könnyebben azonosíthatók a gyanús tevékenységek. Ennek köszönhetően az illetékes szakemberek rövid idő alatt észlelik, ha egy alkalmazott (vagy az online személyazonossága mögé bújt támadó) olyan rendszerekbe lép be, olyan bizalmas fájlokat és adatokat nyit meg, amelyekre nincs szüksége mindennapi munkája során.

Ez természetesen azt jelenti, hogy óriási mennyiségű információt és eseményt kell figyelemmel kísérni. Erről azonban egy fejlett SIEM-megoldás képes automatikusan gondoskodni, ami lehetővé teszi a szakembereknek, hogy csak azokkal az incidensekkel foglalkozzanak, amelyek valóban figyelmet érdemelnek.

Mézescsuprok az AWS-en

Vonzó célpontnak tűnő rendszereket szimuláltak a világ tíz legnépszerűbb AWS adatközpontjában a közelmúltban, s azt találták, hogy ezeket a honeypot felhőszervereket aktiválás után átlagosan 40 percen belül támadták meg először, és percenként átlagosan 13 támadási kísérlet érte mindegyiket. Harminc nap alatt több mint 5 millió támadást számoltak a tíz szerveren, összegzi az eredményeket a Sophos *Exposed: Cyberattacks on Cloud Honeypots* című jelentése. Az eredményekből kitűnik, hogy a digitális bűnözők automatikusan kutatnak gyenge, védtelen felhős tárhelyek után. Amennyiben sikeresen bejutnak, a szervezetek védtelenné válnak az illetéktelen adathozzáférésekkel szemben.

A Sophos szakemberei szerint a publikus felhőinfrastruktúra folyamatos átláthatósága létfontosságú a vállalatok számára ahhoz, hogy tudják, mit kell védeniük, és hogy megfeleljenek a szabályoknak. Az IT-biztonságiak számára azonban komoly probléma, ha a szervezeten belül több fejlesztőcsapat és folyamatosan változó, automatikusan skálázódó környezet van. A nyilvános felhők biztonsági gyengeségeit mesterséges intelligencia használatával lehet orvosolni, az ugyanis képes automatikusan felderíteni a szervezet eszközeit és adatait a nyilvános felhőkben, s ezzel hozzájárul ahhoz, hogy a biztonsági csapatok mindenbe beleláthassanak a felhőn belül, és hogy perceken belül tudják kezelni a biztonsági kockázatokat. Ezen felül a mesterséges intelligencia felderíti a kockázatos erőforrás-konfigurációkat és a gyanús hálózati magatartást is.