HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Póser Valéria, Schubert Tamás, Kozlovszky Miklós, Prém Dániel
poser.valeria@nik.uni-obuda.hu - schubert.tamas@nik.uni-obuda.hu -
kozlovszky.miklos@nik.uni-obuda.hu - prem.daniel@nik.uni-obuda.hu

SECURITY ON-DEMAND MEGOLDÁSOK AZ INFORMATIKAI INFRASTRUKTÚRÁKBAN

Absztrakt

A modern informatika egyre inkább a szükséglet-alapú megoldásokra törekszik. Nincs ez máshogy az informatikai biztonság területén sem. Napról napra jelennek meg új felhőszolgáltatások, amelyeket akár percek alatt használatba lehet venni. Ezzel kielégítve a piac azon igényét, hogy az előfizetők a lehető legtöbb és legjobb szolgáltatásokat a lehető leggazdaságosabban vehessék igénybe szükségletüknek megfelelően. Kutatásunk során megvizsgáltuk a jelenleg elérhető Security as a Service megoldásokat, majd górcső alá vettük azok On-Demand módon történő alkalmazhatóságát, támaszkodva a területen élenjáró Security On-Demand szolgáltató megoldásaira. Cikkünkben ezeket mutatjuk be, külön kitérve olyan témakörökre, mint a sebezhetőség vizsgálat, a behatolás érzékelő rendszer és a tűzfalszabályok és megfelelőség elemzése. A megvizsgált módszerek tapasztalatait pedig felhasználtuk a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 "Kritikus infrastruktúra védelmi kutatások" projekt keretében a saját sérülékenység vizsgálati eszközünk fejlesztése során.

The modern information technology is seeking to use on-demand solutions. This is not different in the field of information security. Day by day appears new cloud based services, which are could be usable within minutes. With this, it satisfies the needs of the market to get the most and the best services, on the cheapest price that is possible. During our research we examined the currently available Security as a Service solutions, and we have looked at their applicability in the way of On-Demand, relying on the Security On-Demand service provider's solutions. In this paper, these solutions will be described and paying special attention to such topics as vulnerability assessment, intrusion detection systems and firewall rules and compliance assessment. The experiences of the examined methods are used in the TÁMOP-4.2.1.B-11/s/KMR-2011-0001 "Critical infrastructure protection research" project, where we develop our vulnerability analysis and assessment tool.

Kulcsszavak: *szükséglet-alapú biztonság, felhő-alapú szolgáltatások ~ Security On-Demand, Cloud Based Sevices*

BEVEZETÉS

A modern szükséglet-alapú számítási megoldás (On-Demand Computing) egyre népszerűbb a nagyvállalatok körében. Terjedésének legfőbb oka, hogy ez a technológia lehetőséget biztosít arra, hogy a számítási erőforrások akkor és olyan mértékben álljanak az ügyfél rendelkezésére, amennyire éppen szüksége van. Azaz, ez a megoldás hatékonyan képes kezelni az erőforrások keresletében bekövetkező ingadozásokat, segítségével elkerülhető, hogy egy adott vállalat informatikai rendszere kihasználatlanul működjön, vagy épp az ellenkezője következzen be, hogy erőforrás hiányában ne legyen képes kiszolgálni a megnövekedett keresletet.

Az erőforrások rugalmas kezelése, mint működési cél, a legjobb szakmai gyakorlat szerinti kritériumok közül a hatékonyságot szolgálják. Elsődleges szempont azonban mindig az intézmény stratégiai céljainak teljesítése. A legoptimálisabb olyan működési biztonság kialakítása, amely a működési célokat a stratégiai célokhoz igazítja [1].

A felhő infrastruktúrákon definiált szolgáltatások napjainkban már lehetővé teszik akár nagyvállalati adatközpontok virtualizált üzemeltetését is. A megfelelő informatikai biztonság kialakításában és fenntartásában jelentős segítséget jelenthet a felhő-alapú biztonság, mint szolgáltatás (Security as a Service - SECaaS) igénybevétele. Segítségével jelentős mennyiségű erőforrás (infrastruktúra, szakértelem, idő, stb.) takarítható meg. Az On-Demand Computing analógiáján jogosan merül fel az igény az igény-szerinti biztonság, mint szolgáltatás igénybevételére is. A SECaaS nagy előnye abban rejlik, hogy szolgáltatási modelljével képes az IT biztonság esetében elengedhetetlenül szükséges szakértelmet az IT erőforrásokkal (hardver és szoftver környezetek) kombinálva hatékonyan elosztani az ügyfelek között maximalizálva a kihasználtságot és ezáltal minimalizálva a költségeket. Ez a koncepció remekül használható nem csak nagyvállalati környezetben, hanem földrajzilag elszórt kisvállalatok esetében.

Kutatásunk során megvizsgáltuk a jelenleg elérhető Security as a Service megoldásokat, és cikkünkben bemutatjuk a legelterjedtebb, legszükségesebb megoldások On-Demand módon történő alkalmazhatóságát. A megvizsgált módszerek tapasztalatait pedig felhasználtuk a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 “Kritikus infrastruktúra védelmi kutatások” projekt keretében a saját sérülékenység vizsgálati eszközünk fejlesztése során.

SZÜKSÉGLET-ALAPÚ BIZTONSÁGI SZOLGÁLTATÁSOK

A vállalatok arra törekszenek, hogy megfelelő védelemmel rendelkezzenek az informatikai rendszereiket érintő fenyegetések, a jogsértések, és a jogosulatlan hozzáférések ellen, ugyanakkor, ahogy a fenyegetések köre átalakul, a hagyományos biztonsági védekezés egyre kevésbé hatékony. Ez azt jelenti, hogy a vállalatoknak más, esetleg további biztonsági intézkedésre van szükségük, amely kiegészíti a meglévő védelmet. Az egyik legfontosabb szükséges képesség egy robusztus biztonsági ellenőrzési és irányítási képesség, amely képes integrálni a különböző biztonsági technológiákat egy olyan elterjedt decentralizált hálózaton is, ahol távol vannak egymástól a telephelyek, a távmunkások, a mobil eszközök, a csatlakoztatott üzleti partnerek.

A kialakult gazdasági válságnak is köszönhetően a vállalatok legfőbb törekvése a lehető legkevesebb ráfordítással a leghatékonyabb biztonság fenntartása. A megfelelési és kockázatkezelési előírások azonban nincsenek tekintettel a válságra, nem szabnak enyhébb követelményeket, mert a vállalatoknak kevesebb anyagi erőforrás áll rendelkezésükre a bizalmas információk védelmére. Az optimális megoldás az informatikai biztonsági funkciók részben, vagy teljes mértékű kitelepítése (outsourcing) lehet. Egyre több kis-és közepes méretű vállalkozás számára ma ez a szolgáltatás sokkal költséghatékonyabb, mintha a

szükséges biztonsági funkciókat teljesen házon belül oldanák meg. Ugyanis, ha a helyzet úgy kívánja, nem kell foglakozni az időközben feleslegessé vagy esetleg szükségessé vált infrastruktúra, vagy szakember problémával, vagy azzal a gonddal, hogy ha egy informatikai munkatársat elveszít a vállalat, akkor elveszti az ellenőrzését olyan technológiák, területek felett, amelyekért korábban az adott munkatárs felelős volt.

Gyakran az informatikai személyzet meglehetősen túlterhelt, gondot okoznak például a következő kérdések:

- személyzet és szakértelem hiánya az informatikai biztonság területén,
- biztonsági események ellenőrzése 7 x 24 órában,
- a legkülönbözőbb biztonsági technológiák kezelése és támogatása,
- teljesítmény és biztonsági naplók ellenőrzése, elemzése,
- a termékek megfelelő konfigurálásához szükséges szakértelem hiánya,
- szoftver licencek és karbantartási szerződések kezelése, stb.

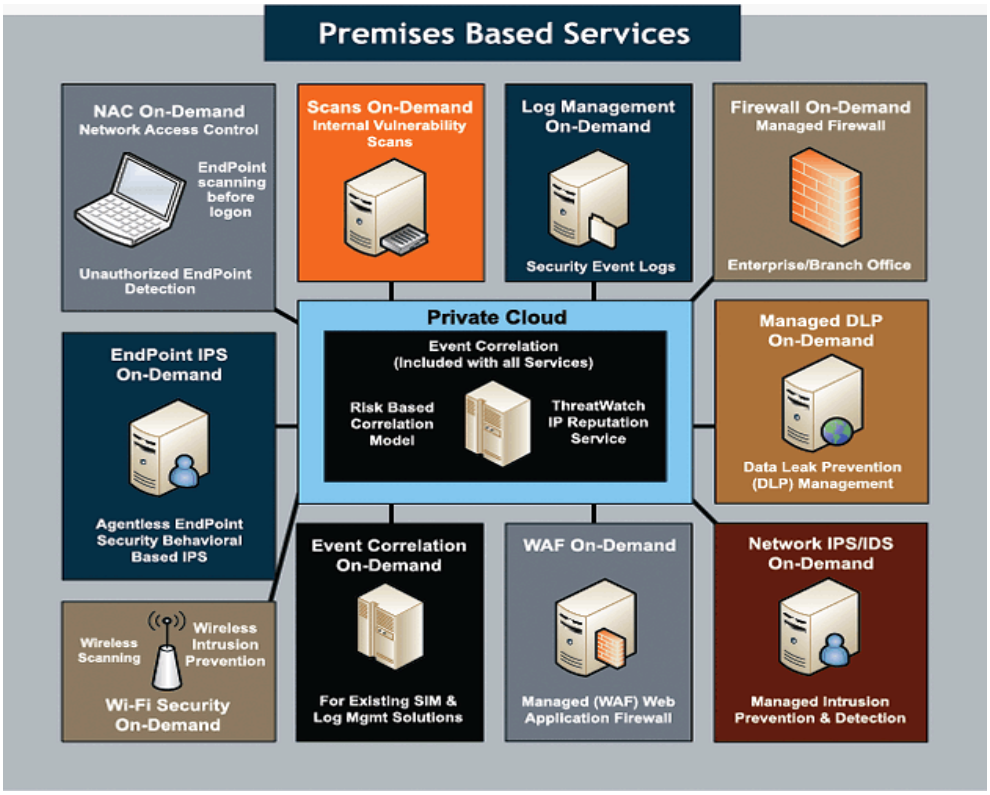
A fenti és hasonló problémák megoldására nyújthat megnyugtató és költségkímélő megoldást a biztonságnak, mint szolgáltatásnak a szükséglet-alapú igénybevétele. Ezért kutatásunk során górcső alá vettük példának okáért a Security On-Demand Társaság által kínált biztonsági megoldásokat.

Security On-Demand lehetőségek

A Security On-Demand nem más, mint a különböző biztonsági szolgáltatások az ügyfelek lehetőségeihez mért és szükségleteinek megfelelő igénybevételi lehetősége. Erre lehetőség van helyileg telepített, felhő-alapú, vagy úgynevezett kevert, vagy hibrid formában.

Telepített szolgáltatások [2]

A telepített biztonsági szolgáltatások (Premises Based Services) célja, a hálózat belső elemeinek integrálása, úgymint a végpontok, szerverek, alkalmazások, biztonsági berendezések és alkalmazások, stb.



1. ábra. Telepített szolgáltatások [2]

Az ebben a formában igénybe vehető biztonsági szolgáltatásokat az 1. ábra szemlélteti, melyek a következők:

1. *Tűzfal menedzselés (Firewall On-Demand):* Csökkenti a vállalat informatikai személyzetének terheit, mert kezel minden tűzfaljelentést, anélkül, hogy egy belső biztonsági szakértőt tartanánk fenn. Különböző megoldás létezik kis- és nagyvállalatok részére, és a különböző típusú tűzfalakat is képes támogatni (pl. Check Point, Cisco, ASA és PIX, Palo Alto tűzfalak, stb.).
   - 24x7 technikai támogatás: többszörösen tanúsított biztonsági és tűzfal mérnökökkel,
   - Compliance & Reporting: segítség a szabályozási követelményeknek való megfelelésben azáltal, hogy azonnal elérhető a tűzfal, valamint biztonsági jelentés készítése arról, amire az informatikai személyzetnek nincs ideje, gyűjtés, kezelés,
   - alacsonyabb költség: kihasználva a Security as a Service megvalósítást, csökken a kezelési és karbantartási költség,
   - ROI: a tűzfal biztonsági frissítéseinek biztosítása, rendszeres karbantartás, állandó biztonsági ellenőrzés, a biztonsági események átláthatósága és a láthatósága a tűzfalon (pl. a Security On-Demand-nál biztonságos internetes portálon naprakész, valós idejű jelentések minden forgalomról, biztonsági eseményekről).

2. *Napló menedzselés (Log Management On-Demand):* A legtöbb napló menedzsment szolgáltatás összegyűjti és összesíti az eseményeket, de valós idejű elemzést nem végez. Azon megoldások esetében, amelyek nem biztosítják ezt a képességet is, külön kell gondoskodni róla, ami jelentős mértékben növeli a költségeket és meghosszabbítja a telepítési és konfigurálási időt. Az a jó napló menedzsment, ami azonnal észleli azokat a biztonsági eseményeket, amelyeket további elemzésre kell küldeni, míg a többi naplót tömöríti archiválás céljából.

3. *Belső sérülékenység vizsgálat (Scans On-Demand):* A Scans On-Demand proaktívan vizsgálja a hálózat sebezhetőségét a belső vagy külső támadásokkal szemben. A vállalatoknak gyakran nincs idejük és erőforrásuk az összes támadási felület felderítésére, mivel a hálózati és alkalmazási környezet állandóan változik, így új támadási felületek keletkeznek. A proaktív sebezhetőség tesztelés és behatolás tesztelés segít felderíteni, hogy hol és hogyan képes a támadó olyan kritikus információkat szerezni a rendszerről, amelyek megkönnyítik a behatolást a külső védelmen keresztül. A sérülékenység menedzsment folyamata hat fontos lépcsőből áll: magában foglalja a hálózaton megtalálható eszközök teljes körű felderítését, ezek osztályozását a könnyebb menedzselhetőség érdekében, a vizsgálat folyamatát, a jelentést, amiből kiderül a kockázat, a sérülékenységek kijavítását, illetve a megfelelő kontrollok bevezetését, valamint a javítások ellenőrzését.

4. *Web Application Firewall (WAF On-Demand):* A valós idejű, folyamatos internetes alkalmazások biztonságát a környezet megfelelő védelme mellett az garantálná, hogy a tervezésük és az implementálásuk kellő körültekintéssel, a megfelelő biztonsági elemek, előírások figyelembevételével történt. Azonban az idő múlásával folyamatosan új sérülékenységek kerülnek napvilágra, amelyek az alkalmazások megszületésekor még nem is léteztek. Ezért fontos, az alkalmazások folyamatos 24x7x365 biztonsági ellenőrzése, hiszen egy új biztonsági rés komoly problémákat okozhat, amelyek akár információszivárgáshoz is vezethetnek. Egy biztonsági hiba utólagos javításának költsége sok esetben csillagászati összegeket emészthet fel, hiszen az alkalmazást akár alapjaiban is módosítani kellhet, és a biztonsági

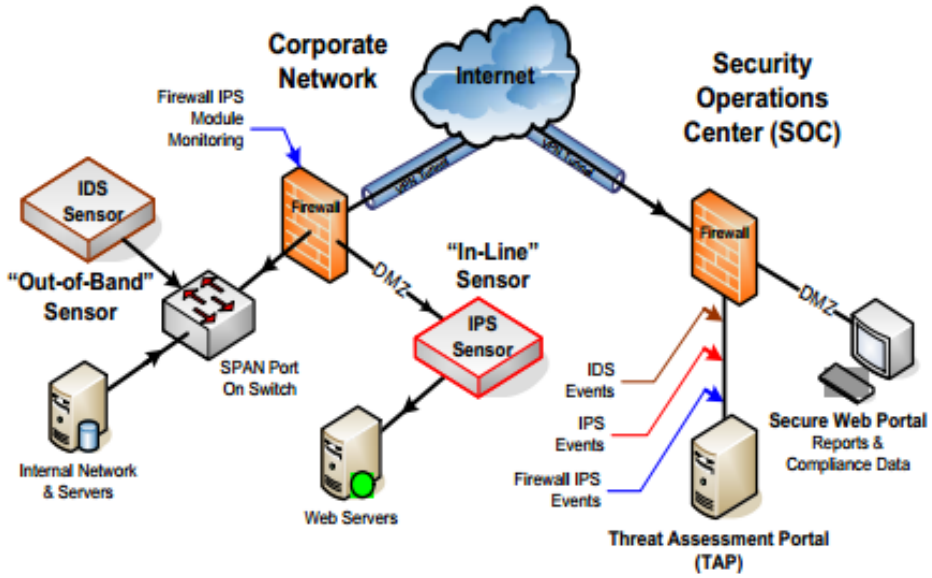
teszteléseket is újra el kell végezni. Emiatt sokkal költséghatékonyabb magoldás lehet egy Web Application Firewall alkalmazása, amelybe csak egy új szabályt kell definiálni a felmerült sérülékenységre.A legtöbb probléma, amiért, és ami ellen védekezni kell:

- a webes alkalmazások az első számú forrása a célzott hacker támadásoknak,
- a célzott alkalmazás támadások általában megkerülik vagy átmennek a tűzfalakon,
- a hálózati biztonsági szkennerek többnyire nem ismerik fel az alkalmazások hibáit, gyengeségeit,
- túl sok a kód és kevés a gyakorlott fejlesztő, aki tudja javítani azokat az alkalmazásokat, amelyek kódja sebezhető,
- az alkalmazások közötti kapcsolat általában bizonytalan.

5. *Wi-Fi biztonság (Wi-Fi Security On-Demand):* A vállalatok hálózati forgalmának egyre nagyobb része „közlekedik a levegőben", és egyre több informatikai eszköz rendelkezik WiFi képességgel, amelyek számos támadási lehetőséget jelentenek. Sok szervezet nem fordít kellő figyelmet és energiát a vezeték nélküli rendszereire, amikor biztonsági technológiát épít ki. A vezetékes hálózatoknál széleskörűen alkalmazott IPS megoldások nem védenek a vezeték nélküli támadások ellen, ezek kezelésére speciális WiFi IPS eszközökre van szükség. A vezeték nélküli behatolás védelmi szolgáltatásnak is folyamatos 24x7 biztonsági ellenőrzésnek kell lenni. A szolgáltatásnak alapos elemzést kell végeznie valamennyi vezeték nélküli csatornára, eszközre, forgalomra. Proaktívan kell azonosítani az összes lehetséges vezeték nélküli fenyegetést, köztük több száz biztonsági rést.

6. *Network Acces Control (NAC On-Demand):* A NAC számos forgatókönyvet tartalmaz a potenciális biztonsági események bekövetkezésekor végrehajtandó lépésekre, amelyek segíthetnek megoldani a valós biztonsági problémákat. Konzultációk alkalmával lehet tisztázni a biztonsági kérdéseket és célokat, amelyek a NAC-ba kerülnek, pl. milyen biztonsági politikát szeretnénk érvényesíteni, milyen megfelelőségi követelményeknek kell eleget tennünk, milyen felhasználói hitelesítés felel meg legjobban számunkra, hogyan kezelje a nem megfelelő felhasználókat, vannak-e illetéktelen hozzáférési végpontok a hálózathoz, stb.

7. *Behatolás jelző rendszer (Network IPS/IDS On-Demand):* A behatolás jelző IDS és IPS szolgáltatás célja, hogy védje a hálózatot a külső és belső támadásoktól. Ma már minden vállalatnak rendelkeznie kell vele, hiszen ez a védelem kritikus pontja. A rosszindulatú adatküldést nehéz kimutatni, mert sokszor téves riasztások is vannak. Ezért nagy szakértelem kell, az ilyen riasztások kiszűréséhez. A behatolás jelző rendszer segít kezelni az információlopás kockázatának észlelését, és meghiúsítja a támadásokat. A megoldás alapja egy 3-rétegű architektúra, amely gazdaságos, kis helyigényű a telepítés, azonban könnyen skálázható nagyszabású telepítések támogatására. Két érzékelőt telepítenek, egy IPS szenzort “in-line” és egy IDS szenzort “out-of-band”, ahogy a következő ábrán látszik.



2. ábra. 3 rétegű architektúra [3]

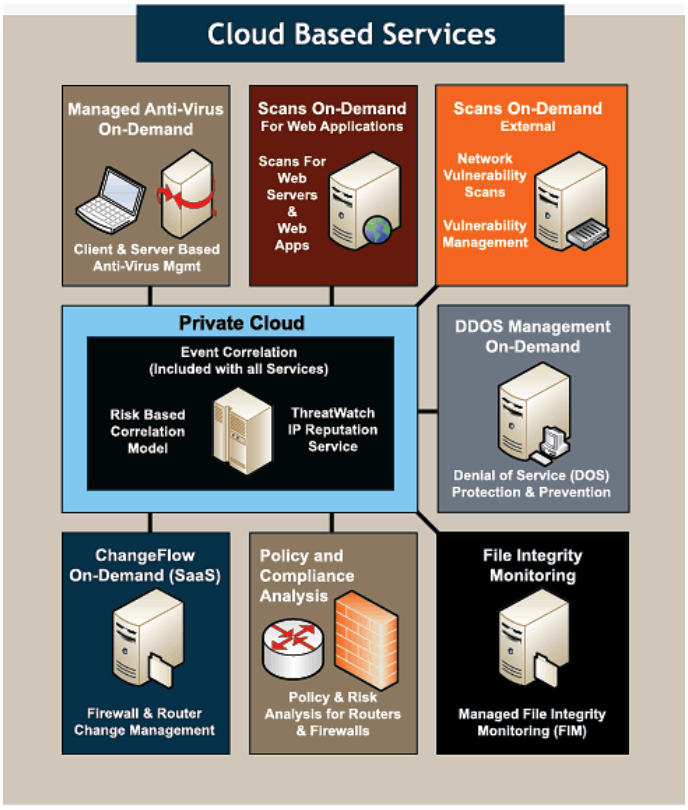
8. *Esemény menedzselés (Event Correlation On-Demand:* Az esemény menedzsment szolgáltatás az informatikai biztonság alapvető építő eleme, egy átfogó szolgáltatás, melynek segítségével csökkenthető a szervezetek üzleti kockázata és működési költsége. A SIM/SIEM rendszerek gyűjtik és elemzik az infrastruktúra, az eszközök, az alkalmazások naplóit, és ha fenyegetést, csalást, vagy visszaélést észlelnek, reagálnak azokra.

9. *Végpont IPS megoldás (EndPoint IPS On-Demand):* Érzékeli a viselkedési anomáliákat, elemzi a végpont együttműködését más rendszerekkel, milyen szolgáltatások futnak az asztalon, észleli a végpont kockázatos magatartását, és ellenőrzi az előre meghatározott végponti politikák végrehajtását. Az ismeretlen felhasználóknak megtagadhatja a hozzáférést attól függően, hogyan van beállítva. Azok a végpontok, amelyek viselkedése sérti a politikát, vagy nem egy vállalati eszköz, korlátozni lehet elkülönítés nélkül, vagy el lehet távolítani a felhasználót a hálózatról. Egyes végponti IPS megoldások képesek felismerni és szétválasztani az ismert és ismeretlen szervezet eszközeinek minden IP alapú eszközét, beleértve a laptopokat, számítógépeket, nyomtató szervereket, forgalomirányítókat, vezeték nélküli hozzáférési pontokat, vagy bármely hálózati eszközt. Előre meghatározott politika alapján az ismeretlen készülékeket vagy felhasználókat, vagy azonnal karanténba teszik, és nem engedik a hálózatra, vagy lehet vendégnek nyilvánítani és csak internet-hozzáférést biztosítani számukra.

10. *DLP megoldás (Managed DLP On-Demand):* A Data Leak Protection (DLP) megoldások egyre elterjedtebbek. Az érzékeny adatok, mint pl. a hitelkártyák, társadalombiztosítási számok, vevőlisták, egészségügyi nyilvántartások, biztosítási információk, címek és más hasonló információk véletlen szivárgásának vagy szándékos kiszivárogtatásának megakadályozására számos eszköz vehető igénybe. Minden megoldás középpontjában az adatosztályozás áll, azaz hogy képesek legyünk meghatározni, hogy milyen típusú adatokat kell megvédeni, és különbséget tenni az ügyfelek adatainak típusai között, mely alapján létre lehet hozni egy politikát a nyomon követésre és az információ szivárgás védelmére. Bár az adatok osztályozása nem elő követelmény, de egy jól definiált adatosztályozási politika kiindulási pont lehet.

Felhő-alapú szolgáltatások [4]

A felhő-alapú biztonsági szolgáltatások (Cloud Based Sevices) kiegészítik a telepített biztonsági szolgáltatásokat, céljuk, hogy integrálják a hálózat külső elemeit, mint pl. a web szerverek, tűzfalak, szerverek, alkalmazások, webes tartalom és sérülékenység elemző eszközök, ezáltal nyújtva olyan átfogó biztonsági stratégiát, amely megvédi a szervezetet az összes lehetséges támadási módszertől.



3. ábra. Felhő-alapú szolgáltatások [4]

Az ily módon igénybe vehető biztonsági szolgáltatásokat a 3. ábra szemlélteti, melyek a következők:

1. *Vírusvédelem (Managed Anti-Virus On-Demand):* Az informatikai rendszerek és azon keresztül a vállalatok zökkenőmentes működésének egyik kritikus pontja a vírusvédelem. Ha az aktuális frissítés nem töltődik le időben, abból katasztrófa alakulhat ki. A víruskereső rendszerek log adatainak gyűjtését és figyelemmel kísérését legtöbbször figyelmen kívül hagyják a szervezetek. A megoldás lényege, hogy a beépített vírusvédelemnek köszönhetően a riasztási üzenetek, figyelmeztetések a szolgáltató rendszerébe valós időben futnak be, ahol képesek megfelelően kezelni azokat. A szolgáltatás figyeli, hogy a víruskereső frissítési fájlok megfelelően letöltődtek-e, továbbá támogatja a kártevőirtókat (anti-malware), kémprogram irtókat (anti-spyware), együttműködik a helyileg telepített vírusvédelmi termékkel. Teljes nyilvántartást vezet minden riasztásról, vizsgálatról és válaszról.

2. *Webes alkalmazások sebezhetőségének vizsgálata (Scans On-Demand for Web Applications):* A felhasználók korlátozására lehet tűzfalakat használni, azonban a tipikus HTTP és HTTPS protokollokra korlátozott forgalom is hordozhat olyan kódot, amely kihasználhatja a webes alkalmazásokban lévő sebezhetőségeket. Az ilyen sebezhetőségek kihasználása vezethet adat szivárgásához, a webes oldal eltorzításához, vagy más támadásokkal akár kompromittálhatják a létfontosságú

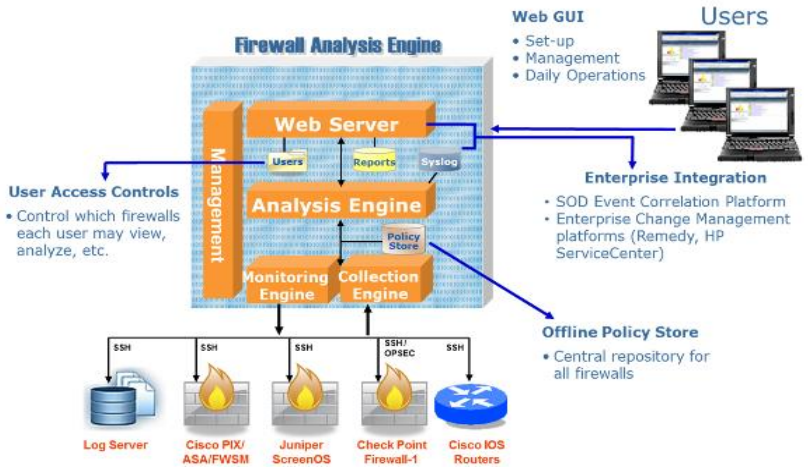
adatok integritását és titkosságát. Legyen szó bármilyen méretű vállalkozásról, ha saját magunk üzemeltetjük a webes alkalmazásainkat, nem árt biztosítanunk a weboldalainkat az alkalmazás szintű fenyegetettségek ellen. A Scans On-Demand for Web Applications szolgáltatás a webes alkalmazásokat és webhelyeket távolról értékeli, a sérülékeny pontokat azonosítja, majd blokkoló szabályokat hoz létre a Web Application Firewall-on (WAF) a feltárt sebezhető pontok alapján.

3. *Hálózati sérülékenység menedzsment (Scans On-Demand External):* A szolgáltatás segítségével proaktív módon azonosíthatók és kiküszöbölhetők a hálózat és összetevőinek sérülékenységei. Korrelálja a sérülékenység vizsgálati adatokat, valós időben elemzi a különböző forrásokból érkező biztonsági eseményeket, beleértve a hálózatot alkotó gépek, szerverek, hálózati eszközök, alkalmazások, adatbázisok, stb. biztonsági naplóit.

4. *DDoS támadás elleni védelem menedzselése (DDoS Management On-Demand):* A DDoS támadás például úgy keletkezik, hogy egy automatizált eszköz (alkalmazás) felkutatja az internetre kapcsolódó sebezhető számítógépeket. Amikor talál olyat, melyet képes megfertőzni, feltelepít egy rejtett támadóprogramot, melynek segítségével távolról vezérelhetővé válik egy „mester" gépről (a támadó gépéről). Ha elég gépet fertőzött meg a támadóprogrammal a „mester" állomás jelt ad a „zombiknak", hogy kezdjék meg a támadást a kiszemelt célpont vagy célpontok ellen. Ekkor az összes „zombi" egyszerre elindítja a támadást, és bár egyenként kis mennyiségű adattal dolgoznak, mégis több száz, vagy akár százezer támadó gép esetén a sok kis adatcsomag eredménye hatalmas adatáramlás, mely a megtámadott gép, vagy rendszer ellen irányul. Ha a DDOS Management eszközök visszaélést fedeznek fel, azonosítják a támadót, és kiejtik a támadó forgalmat, állomást vagy tartományt.
5. *Fájl integritás monitorozása (File Integrity Monitoring):* Ez a szolgáltatás a napló menedzsment része, azoknak az eseményeknek a felderítésére szolgál, melyeket a hagyományos napló menedzsment, vagy monitorozó rendszerek, mint a SIM/SIEM rendszerek nem képesek felderíteni. A rendszer konfiguráció, a fájlok, könyvtárak változását monitorozza.

6. *Tűzfalszabályok és megfelelőség elemzés (Policy and Compliance Analysis On-Demand):* Egyedi tűzfalak, tűzfal csoportok, vagy Cisco IOS alapú forgalomirányítók esetében a biztonsági politikák beállításainak ellenőrzésére szolgál. Az elemzés offline módon történik. Átfogó, jól méretezhető, egyszerűen telepíthető és használható szolgáltatás, ami támogatja az elérhető jelentősebb nagyvállalati tűzfal platformokat.

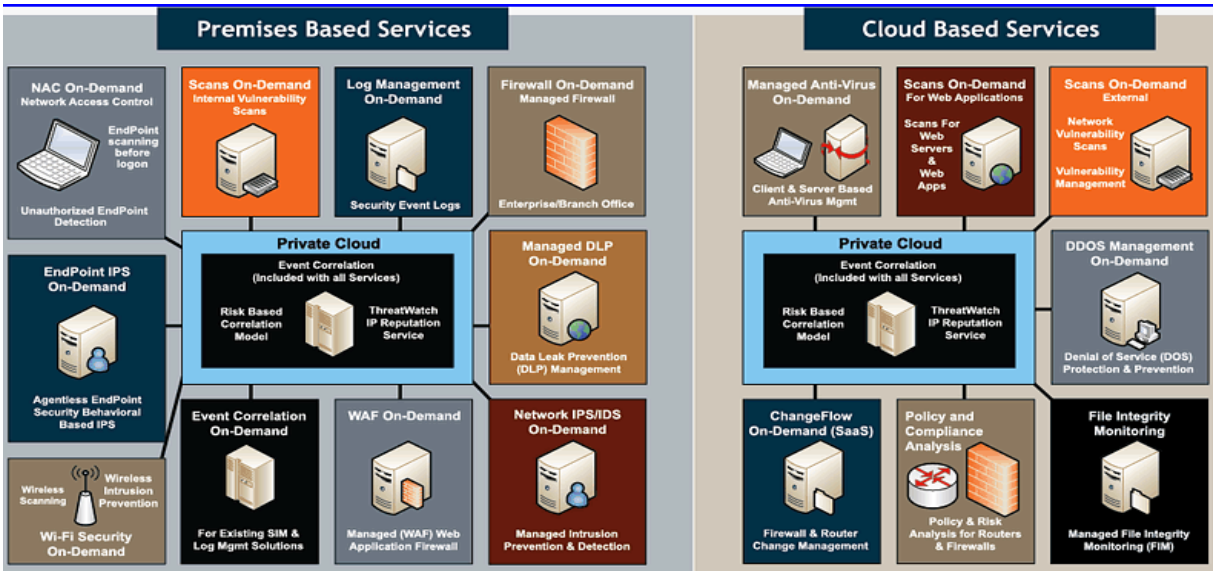
7. *Változás menedzselés (ChangeFlow On-Demand):* A szolgáltatás tűzfalak és forgalomirányítók automatizált változás menedzsment eszköze.



4. ábra. Policy and Compliance Analysis [5]

Hibrid biztonsági architektúra [6]

A hibrid vagy kevert biztonsági architektúra (5. ábra) kihasználja mindkét biztonsági architektúrának (telepített és felhő-alapú) az előnyeit.



5. ábra. Hibrid biztonsági architektúra [6]

A két szolgáltatás típus együttes alkalmazása biztosítja a legjobb telepíthetőséget, szállíthatóságot, és menedzselhető mind a szolgáltató, mind az ügyfél oldalon. Az eredmény egy rendkívül jól méretezhető hibrid biztonsági architektúra, amely nem igényel tőkebefektetést, és enyhíti az informatikai személyzet terheit, 24x7 lefedettséget és menedzsmentet biztosít.

A SECURITY ON-DEMAND MEGOLDÁS ELŐNYEI, ALKALMAZHATÓSÁGA

Az On-Demand felhő-alapú biztonsági szolgáltatások előnyeinek jelentős része a Security as a Service megoldásból származik, és csak bővíti az előnyök körét, hogy ezen szolgáltatások igénybevétele kivitelezhető úgy is, hogy a szolgáltatás díját csupán a valós szükségletnek és lehetőségeknek megfelelően kell megfizetni.

A legfontosabb előnyök tehát:

- *Megszünteti a technológiai tanulási görbét:* egy tipikus szervezet, amikor saját eszközökbe és rendszerekbe fektet be, gyakran tapasztal meredek tanulási görbét a tervezés, a végrehajtás, a konfiguráció terén. Azáltal hogy a szolgáltatás igénybe vétele megszünteti, vagy jelentős mértékben csökkenti az alkalmazottak tanulási görbéjét, a szervezet támogatására, az üzleti műveletekre tudnak összpontosítani.
- *Telepítés gyorsasága:* a technológia kiépítése, az informatikai környezet integrálása meglehetősen költséges. Általában a szolgáltatás teljes telepítése és hangolása kevesebb, mint 30 nap, így felgyorsítja a befektetések megtérülését az ügyfél számára.
- *Költségek (beruházások, szolgáltatási színvonal fenntartása, licencek):* jelentős összeget és folyamatos ráfordítást vesz igénybe a szükséges környezet, az infrastruktúra kialakítása és folyamatos karbantartása, fejlesztése. Számos szervezet nem is rendelkezik kellő anyagi forrással, és nem is lenne gazdaságos a biztonsági szolgáltatások saját kivitelezése. A Security On-Demand biztosítja és fenntartja az összes hardver, szoftver, licencek támogatását, ezek beszerzésére, beüzemelésére, karbantartására, fejlesztésére nem kell erőforrásokat allokálni.
- *Csökkenti a technológiai kockázatot:* költséges technológia beszerzése azzal a kockázattal jár, hogy nem elégíti ki maradéktalanul az elvárásokat. Ekkor a váltás is igencsak költséges. A Security On-Demand megszünteti ezt a kockázatot, minimalizálja a beruházást, az ügyfél a szolgáltatói szerződés megkötése előtt kipróbálhatja a biztonsági technológiát. Ezen kívül lehetőség van a megállapodás megváltoztatására, átalakítására, vagy megszüntetésére, ha a szolgáltatás nem felel meg az elvárásoknak.
- *Személyzeti és biztonsági szakértelem:* nem szükséges vagy lényegesen kisebb mértékben szükséges a megfelelő szaktudású munkatársak alkalmazása, kiképzése. A Security On-Demand kiküszöböli a fluktuáció veszélyét, és megszünteti a képzés költségeit, garantálja a szolgáltatás folyamatosságát.
- *Rugalmas kapacitás tervezés:* lehetővé teszi, hogy az ügyfél csak a ténylegesen igénybe vett szolgáltatásokért fizessen, a körülményekben bekövetkezett változások, legyen az növekedés vagy visszafejlődés, a szolgáltatások köre és mértéke rugalmasan változtatható.
- *Lefedettség:* csak a legnagyobb vállalatok engedhetik meg maguknak, hogy biztonsági szakemberek a nap 24 órájában készenlétben legyenek a biztonságot érintő események figyelésére és az incidensek elhárítására. Ennek hiányában a szervezetek vagy figyelmen kívül hagyják azokat a biztonsági eseményeket, amelyek nem munkaidőben keletkeztek, vagy az informatikai személyzet osztályozza a biztonsági eseményeket, és órák után kerülnek a figyelmeztetések továbbításra. Mindkét stratégia jelentős kockázatot jelent a szervezetnek azáltal, hogy nagy a munkaidőn kívüli lefedetlen idő rés. A Security On-Demand redukálja ezt a kockázatot, a szolgáltatások igény esetén 24x7x365 elérhetőségűek.

A Security On-Demand alkalmazhatósági területei:

- *Kis- és közepes méretű vállalkozások:* A technológia ebben a szektorban alkalmazható leginkább, mivel az általa biztosított szolgáltatások itt biztosítják költséghatékonyan a megfelelő biztonságot (szakértelem hiány megszüntetése, rugalmas, igényekhez igazodó infrastruktúra és szolgáltatás igénybevételi lehetőség, stb.)

- *Pénzügyi szolgáltatók:* Talán ebben a szektorban a legjelentősebb a különböző szabályozásoknak való megfelelés. Vannak azonban többszörös és egymást átfedő szabályozó testületek, szabványok, irányelvek, jogi követelmények és közzétett iránymutatások, amelyek között esetenként nincs szinkron. Ilyen előírások és követelmények beépítésével az On-Demand biztonsági szolgáltatások közé, jelentősen megkönnyíthető e szervezetek biztonságos működése.
- *Egészségügy és kapcsolódó vállalatok:* A Security On-Demand az egészségügyi ágazatban a következőképpen néz ki: Biztonságosan elérhetővé teszi a létfontosságú IP alapú egészségügyi felszereléseket és számítástechnikai eszközöket, védi a külső és belső hálózatot a jogosulatlan használattól vagy a hozzáféréstől. Segíti a megfelelést a HIPAA követelményeknek. Visszajelzést ad a vállalati adatvagyon jogosulatlan elérési kísérletekor. Észleli a rosszindulatú programokat, beleértve a nulladik napi (zero day) fenyegetéseket, botneteket, keyloggereket, trójaiakat, férgeket és vírusokat.
- *Kormányzati kritikus infrastruktúrák és oktatás:* A kormányzati és más közintézmények is egyre nagyobb mértékben szembesülnek biztonsági fenyegetésekkel, azonban gyakran itt áll rendelkezésre a legkevesebb forrás a megfelelő védelem kialakítására, fenntartására. A kritikus infrastruktúrák sok esetben egységesített, illetve ezeken felüli speciális biztonsági megfelelősségekkel rendelkeznek. Ezek központosított, megfelelő szakmai színvonalú ellenőrzése költséghatékonyságot és magasabb minőséget eredményezhet. Azonban a technológia még viszonylag gyerekcipőben jár, nem kellő mértékű szabályozottsága, és nem utolsó sorban az adatok határokon átnyúló akár csak ideiglenes tárolása (esetleg más szabályozás van érvényben) óvatosságra int ebben a szektorban.

ÖSSZEGZÉS

A vállalatok, szervezetek számára a felhő technológiák alkalmazása nem csak költségvetési szempontból előnyös, hanem az informatikai rendszereik biztonsági előírásoknak, szabványoknak való megfelelőségi szintje is jelentősen javul. Nagyobb mértékben tudnak az alapvető üzleti tevékenységeikre koncentrálni, mivel kihelyezhetik azokat a rutinfeladatokat, amelyek csak megterhelik a költségvetést, de nem hoznak többletértéket, és így biztosak lehetnek abban, hogy valamennyi törvényi, megfelelőségi előírásnak eleget tesznek. A szolgáltatásokat biztosító szolgáltató szervezetek megbízhatóságának garantálása az egyik sarkalatos pontja a biztonsági feladatok kihelyezésének, virtualizálásának. A szolgáltató működésének megfelelő átláthatósággal, ellenőrizhetőséggel kell rendelkeznie, melyeket szigorú, folyamatosan ellenőrzött tanúsítványokkal kellene igazolni.

KÖSZÖNETNYILVÁNÍTÁS

A szerzők ezúton mondanak köszönetet a TÁMOP-4.2.1.B-11/2/KMR-2011-0001 „Kritikus infrastruktúra védelmi kutatások” projektnek a cikkhez végzett kutatások anyagi támogatásáért. A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Felhasznált irodalom

[1] K. Szenes: Operational Security - Security Based Corporate Governance, in Proc. of IEEE 9th International Conference on Computational Cybernetics, July 8-10, 2013 Tihany, Hungary, pp. 375-378, IEEE Catalog Number: CFP13575-USB (pendrive); CFP13575-PRT (printed), ISBN: 978-1-4799-0061-9 (pendrive); 978-1-4799-0060-2 (printed)

[2] Security On-Demand: Premises-Based Security Services, http://www.securityondemand.com/Services/PremisesSecurity/index.htm, 2013.05.16

[3] Security On-Demand: Intrusion Monitoring On-Demand, http://www.securityondemand.com/images/datasheets/IM.pdf, 2013.06.06

[4] Security On-Demand: Cloud-Based Security, http://www.securityondemand.com/Services/CloudSecurity/index.htm, 2013.06.23

[5] Security On-Demand: Firewall Policy and Compliance Analysis http://www.securityondemand.com/Services/CloudSecurity/PolicyAndCompliance.htm, 2013.07.15

[6] Security On-Demand: Security Architecture Overview http://www.securityondemand.com/SolutionCenter/SecurityArchitecture.htm, 2013.07.15