

McAfee®

McAfee teljes körű védelem

A kockázatkezelés élelciklusa

A kritikus vállalati eszközök védelme



Tartalomjegyzék

Áttekintés	3
Diagram (tízlépéses kockázatkezelési életciklus)	4
I. ELSŐ LÉPÉS: HÁZIREND	5
II. MÁSODIK LÉPÉS: LETÁR	5
III. HARMADIK LÉPÉS: PRIORITÁSOK FELÁLLÍTÁSA	6
IV. NEGYEDIK LÉPÉS: SÉRÜLÉKENYSÉGEK	7
V. ÖTÖDIK LÉPÉS: FENYEGETÉSEK	8
VI. HATODIK LÉPÉS: KOCKÁZAT	8
VII. HETEDIK LÉPÉS: BLOKKOLÁS	9
VIII. NYOLCADIK LÉPÉS: HELYREÁLLÍTÁS	10
IX. KILENCEDIK LÉPÉS: MÉRÉS	11
X. TIZEDIK LÉPÉS: MEGFELELŐSÉG	12
Összefoglalás	13

Áttekintés

Teljes körű védelem

A vállalatok vagy kormányzati szervek kritikus eszközeinek megfelelő védelme érdekében a megbízott biztonsági szakembereknek teljes mértékben tisztában kell lenniük a kockázatokkal még azelőtt, hogy bármiféle, az erőforrások hatékony védelmét szolgáló megoldást kidolgoznának.

Jelen dokumentum egy a kritikus területeket azonosító, tíz lépésből álló kockázatkezelési életciklust ismerteti, amelynek segítségével hatékony kockázatkezelési program hozható létre vállalatmérettől és iparágtól függetlenül. A dokumentum azon specifikus kutatásokkal, stratégiákkal és technológiákkal foglalkozik, amelyek hálózatuk biztonságosabbá tételével segítenek a szervezetek számára csökkenteni kockázataikat.

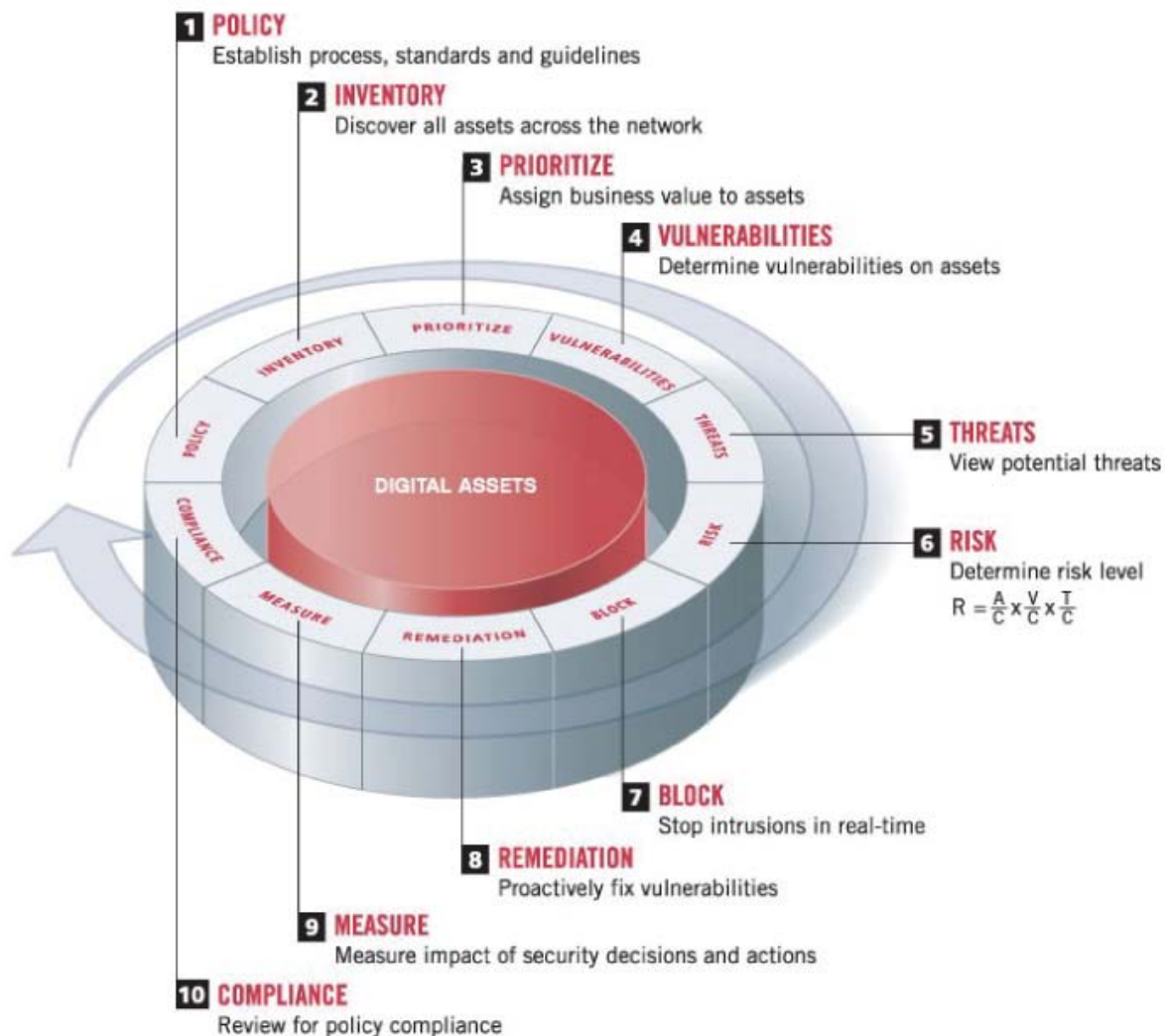
Bár számos szervezet alkalmaz olyan biztonsági megoldásokat, mint a tűzfalak vagy a vírusirtó programok, ezen próbálkozások önmagukban nem elegendőek a létfontosságú infrastrukturális összetevőknek a folyton változó belső és külső (Internet) fenyegetésekkel szembeni védelmére.

Kockázataik maximális megismerése és az életciklus egyes lépéseinek alkalmazásával bármely szervezet képes információbiztonsági program alkalmazására a digitális eszközeikkel szembeni legújabb fenyegetések kivédése érdekében.

Az életciklus valamennyi lépését az adott szervezet követelményeihez és irányelveihez lehet és kell is igazítani, azonban egyik lépést sem tanácsos kihagyni vagy nem a megfelelő sorrendben teljesíteni.

Az életciklus egyes lépéseinek bemutatása során az adott lépés sikeres teljesítéséhez alkalmazható McAfee-technológiákat és -megoldásokat is ismertetjük.

A kockázatkezelés életciklusa



Tízlépéses kockázatkezelési életciklus

I. Első lépés: HÁZIREND

A hatékony biztonsági irányelvek alapvető fontosságúak a vállalat digitális eszközeit célzó fenyegetések csökkentése vagy felszámolása érdekében.

- Stratégia – A hatékony biztonsági program célkitűzéseinek megértése, valamint annak maximális belső támogatása (beleértve a kikényszerítéshez való jogot is).
- Folyamat – Az irányelvek szervezeten belüli kezelésének, valamint a betartásuk módjának megértése. Eljárások és folyamatok kidolgozása az irányelvek be nem tartása és a biztonsági incidensek kezelésére.
- Szabványok és irányelvek – Bevett szabványok beépítése az irányelvekbe, valamint az irányelvek által támogatott és érvényesített új szabványok meghatározása.
- Az irányelvek kommunikálása – Ez a legfontosabb lépés magában foglalja az irányelvek által érintett felhasználók oktatását, annak biztosítását, hogy tudják, hol található meg az irányelveket, mit kell tenniük és kit kell értesíteniük a szabályok megsértése vagy biztonsági incidensek esetén.
- Megbízható rendszerek alkalmazása – Ez a lépés megakadályozza, hogy a felhasználók az irányelvek által nem engedélyezett szoftvereket telepítsenek, nem biztonságos konfigurációs változtatásokat kezdeményezzenek vagy a szabványos, jóváhagyott konfigurációtól eltérő elemeket adjanak a rendszerhez.

McAfee ePolicy Orchestrator® (ePO)

Az ePO megfelelő alkalmazásával a szervezet képes progresszív irányelvek és megfelelési funkciók alkalmazására a bevett irányelvek, valamint a megbízható rendszerekkel kapcsolatos szabványok ellenőrzése és betartása érdekében. Az ePO által szolgáltatott adatok segítenek továbbá az irányelvek hatékonyságának mérésében is.

- System Compliance Profiler (SCP – a javítócsomagok verziójának ellenőrzése) – Az ePO szerves részét képező SCP az operációs rendszer kritikus javítócsomagjainak, valamint az általános működési környezetnek az alapvető megfelelési ellenőrzését végzi.
- Rogue System Detection (idegen rendszer észlelés) – Ezen funkció azáltal javítja az irányelvek vállalaton belüli megfelelését, hogy azonosítja az idegen (az ePO által nem monitorozott) vagy védelem nélküli rendszereket, és lehetővé teszi az ePO számára, hogy az adott rendszerből biztonsági elveken alapuló választ váltson ki.

II. Második lépés: LETÁR

Miután a biztonsági irányelveket kialakította, az eredményesség érdekében a szervezetnek maximálisan tisztában kell lennie megóvandó digitális eszközeivel. Az átfogó kockázatkezelési program legjobb gyakorlatainak megvalósítása érdekében az érintett eszközöknek az alapvető „üzleti folyamathoz” szükséges, könnyen meghatározható eszközökön túl magukban kell foglalniuk minden hálózatot, szegmenseket, rendszert, felhasználót és alkalmazást. A Foundstone Vulnerability Management nevű McAfee termék célja, hogy adatokat szolgáltatson a sikeres leltárhoz. A Foundstone megfelelő alkalmazásával a szervezet pontosan meghatározhatja a számítástechnikai és hálózati környezetében található valamennyi eszközt, feleslegessé téve ezzel a becslést. Időszakos ellenőrző vizsgálat beütemezésével a szervezet az új eszközöket közvetlenül telepítésüket követően képes észlelni, nem kell az időszakos auditokat megvárnia. A Foundstone

Vulnerability Management megoldás maximálisan skálázható, emellett alapvető fontosságú ezen lépés sikeressége, valamint az életciklus egésze szempontjából.

McAfee Foundstone

Gazdaszámítógép leltár – A Foundstone host (hálózatba kapcsolt számítógép) észlelési funkciója azonosítja a hálózatban található (azaz IP címmel rendelkező) valamennyi eszközt. Ez a technika nem csak az olyan hagyományos eszközök széles skáláját fedi le, mint a szerverek, routerek és adatbázisok, de egyéb nem hagyományos eszközöket is magában foglal, amelyek szintén csatlakoztatva vannak az internetre, mint például a specializált ellenőrző rendszerek és az egyéb testre szabható hardverek.

McAfee ePolicy Orchestrator

- Microsoft Active Directory (címtár) integráció – A rendszerek menetrendszerinti importálása az AD-ből az ePO katalógusába az AD tároló objektumok rendszeres lekérdezése révén, amelynek célja a hálózathoz adott új rendszerek észlelése.
- Rogue System Detection (idegen rendszer észlelés) – Az ePO elosztott érzékelőinek segítségével folyamatosan és valós időben ellenőrzi a helyi hálózatba kapcsolt új hálózatokat és megállapítja az idegen rendszer igen/nem státuszát. Az ePO ezt követően többféle manuális és/vagy automatikus választ küld az idegen rendszerről, ezek a következőket foglalják magukban: azonnali értesítés az idegen rendszer kapcsolódásáról, az ePO kliens telepítése, a kivétel megjelölése és harmadik fél által fejlesztett eszköz használata.

III. Harmadik lépés: PRIORITÁSOK FELÁLLÍTÁSA

A sérülékeny eszközök meghatározását követően fel kell állítani a prioritási sorrendet. A sorrend felállításakor a következő kérdéseket kell figyelembe venni:

- **Érték** – Nem tényleges költség, hanem az állásidő és a helyreállítás költsége. Például egy ügyfelekkel foglalkozó, bevételeket generáló webes alkalmazás, vagy egy olyan alkalmazás esetében, amelynek működése elengedhetetlen valamilyen bevételt hozó szolgáltatáshoz, a költséget az állásidőből eredő bevételkiesés jelenti.
- **Incidens helyreállításának költsége** – Ha történt korábban valamilyen incidens, mennyibe került az állásidő és mennyibe a helyreállítás? Sasser vagy Slammer féreg, vagy esetleg valami vírus okozta a kárt? Ezek mind jó alapul szolgálhatnak az ezt a lépést gyakran kísérő becslések során.
- **Kieső termelőképesség** – Ez tartalmazza az adatvisszanyerés költségeit, azon időmennyiséget, amíg egy adott kritikus felhasználó vagy csoport kapcsolat nélkül marad (offline), azon időmennyiséget, amíg az ügyfelek nem tudják elérni az oldalt, és az új alkalmazások késedelmes szállításából eredő költségeket, stb.
- **A működésre gyakorolt hatás** – Erre lehet példa a rendszer helyreállításának azon költsége, amely ténylegesen nem a biztonsági csoportot érinti. A kémprogramok például idővel lassíthatják a rendszer válaszadási idejét, a help deskhez érkező hívások száma megnő, és végül az egyetlen helyreállítási lehetőség az, hogy adott felhasználót kiiktatják a hálózathoz és újratelepítik a fertőzött rendszert. Ez az a pont, ahol a felhasználói prioritás fontossá válik.
- **Az üzleti folyamatok feltérképezése** – Például az ügyfelekkel foglalkozó webes alkalmazás és azon adatbázis közötti kapcsolat, amelyre az alkalmazás támaszkodik az ügyfelek kiszolgálása során. Ez a lépés ijesztőnek tűnhet, azonban az eszközök teljes leltározása és értékelése létfontosságú a vállalati rendszereknek a fejlesztési

rendszerekkel, illetve az ügyfeladatoknak a nem-ügyfeladatokkal szembeni hatékony rangsorolása szempontjából.

McAfee Foundstone

- **Eszközök osztályozása** – A Foundstone program eszközosztályozási funkciójának alkalmazásával a szervezet részletes és rugalmas kritériumok alapján osztályozhatja rendszereit. Ez lehetővé teszi olyan tulajdonságok hozzárendelését az eszközökhöz, mint az eszköz tulajdonosa és kritikussága, amelyek segítségével az eszközértékek a vállalati igényekhez hangolhatóak.
- **Eszközalapú sérülékenység-kezelés** – Ez a funkció lehetővé teszi a szervezet számára, hogy a legfontosabb rendszerek helyreállítására fókuszáljon.
- **Az ePolicy Orchestrator-ral történő integráció** a jövőben összetettebb eszközrangsorolást, valamint a termékek és a kapcsolódó adatforrások közötti információ-megosztást tesz lehetővé.

IV. Negyedik lépés: SÉRÜLÉKENYSÉGEK

Ez a lépés néha zavarba ejtő szokott lenni, mivel sok szervezet gyakran egyformán kezeli az összes sérülékenységet. A sérülékenységek megfelelő kezelésének egyetlen módja, ha ismerjük a hálózat valamennyi kritikus eszközét, megfelelően rangsoroljuk azokat és felfedezzük sérülékenységeiket. Ami a felszínen úgy tűnik, mint több rendszerben egyszerre előforduló egyazon sérülékenység, valójában több, egészen különböző sérülékenységet is takarhat. Ezen lépés megfelelő megközelítésének értelmezése és teljes körű alkalmazása segíti a legkritikusabb eszközök azonosítását.

A sérülékenységekkel kapcsolatban szerzett információk és az eszközök rangsorolásának egyensúlyba hozásával a szervezet megfontoltan állhat hozzá a helyreállításhoz. A teljes életciklust követve vége azoknak az időknak, amikor több kötetnyi értékelési jelentést kellett a rendszeradminisztrátor kezébe nyomni. A legnagyobb hatás elérése érdekében azonban ezt a lépést a következő lépéssel, a FENYEGETÉSEK megnevezésével kell kombinálni.

A McAfee ePO segít a sérülékeny eszközök azonosításában

- **Rogue System Detection (idegen rendszer észlelés)** – Ezen funkció célja a vállalatban belüli irányelvek megfelelőségének javítása az idegen és védelem nélküli rendszerek azonosítása révén, valamint azáltal, hogy lehetővé teszi az ePolicy Orchestrator számára, hogy irányelveken alapuló választ váltson ki az adott rendszerből. Egy nem megfelelően konfigurált vagy nem biztonságos rendszer kritikus sérülékenységeket idézhet elő a hálózatban. A McAfee ePO Rogue System Detection segíti a nem megfelelő rendszerek ellenőrzését a hálózathoz történő csatlakozástól kezdve.

McAfee Foundstone

- **Sérülékenység-kezelés** – A Foundstone egy komplett sérülékenység-kezelő rendszer, amely lehetővé teszi a szervezet számára a felfedezett eszközök üzleti érték szerinti rangsorolását, valamint hogy a helyreállítási tevékenységeket elsőként a legkritikusabb rendszereken végezhesse el.
- **Automatikus sérülékenység-frissítés** – Az automatikus sérülékenység-frissítés funkció révén a szervezet képes gyorsan meghatározni infrastruktúrája érintett rendszereit, amint az új sérülékenységeket felfedezik és bejelentik a nyilvánosság számára.

- A sérülékenységek pontos felderítése – A sérülékenység-ellenőrzések és a meghatározott operációs rendszeren, nyitott portokon és protokollokon alapuló gép összepárosításával a Foundstone több mint 3000 sérülékenységet képes biztosan felismerni.

V. Ötödik lépés: FENYEGETÉSEK

Gyakran előfordul, hogy egy szervezet széles körben hoz rendbe sérülékenységeket anélkül, hogy teljesen tisztában lenne az eszköz értékével vagy a fenyegetésekkel. Ez a lépés nem csak a fenyegetés megismerését foglalja magában, hanem annak tisztázását is, hogy hatásos lehet-e, és ha igen, hogyan, egy potenciális sérülékenységeken alapuló környezetben. Ez az utolsó lépés a valós kockázati szint meghatározása során, amely segíti az adott környezet potenciális fenyegetéseinek és azoknak az eszközökre gyakorolt hatásának felderítését.

A legsérülékenyebb és legkritikusabb eszközökre lefelé, a második lépéstől a negyedik lépésig terjedő szakaszban a McAfee ePolicy Orchestrator és a McAfee Foundstone segítségével felderített és rangsorolt fenyegetések megismerésével a szervezet képes lesz az adott problémához megfelelő védelmi technológia bevetésére és a probléma kezelésére.

McAfee Foundstone Threat Correlation Module (fenyegetés megfelelés modul)

A Threat Correlation Module percre kész fenyegetés felderítési riasztásokat ad a McAfee Research-től, amely lehetővé teszi, hogy a szervezet azonnal reagáljon az olyan bekövetkező eseményekre, mint a férgek vagy egy nagyszabású támadás. A Threat Correlation Module kockázati besorolást rendel minden egyes fenyegetéshez az eseményeknek a vállalat eszközeihez és a sérülékenységekkel kapcsolatos információihoz való viszonyában. A szervezet, felhasználva ezt az információt gyorsan reagálhat akkor és ott, amikor és ahol a legkritikusabb eszközök veszélyben vannak.

Foundstone's Threat Compliance View (fenyegetés megfelelési vizsgálat)

Automatikusan nyomon követi és grafikusán ábrázolja a szervezet fenyegetésre adott válaszát üzleti egységenként és platformonként, szemben a bevett helyreállítási célokkal vagy irányelvekkel. Ez a korszerű műszerfal-nézet (dashboard) értékeli és elemzi a fenyegetésre adott válaszokat annak érdekében, hogy a biztonsági menedzserek nyomon követhessék, ahogyan csapatuk helyreállítási eljárása semlegesíti az adott fenyegetést.

VI. Hatodik lépés: KOCKÁZAT

Az alábbi formula, illetve az elsőtől az ötödik lépésig terjedő szakaszokból származó adatok felhasználásával a biztonsági menedzser képes megfelelően felmérni a szervezet sérülékeny eszközeire lefelé kockázatok valós szintjét.

$$R = \frac{A}{C} \times \frac{V}{C} \times \frac{T}{C}$$

R/K = Risk / Kockázat

A/E = Asset Value / Eszközérték

V/S = Vulnerability Severity / A sérülékenység súlyossága

T/F = Threat Criticality / A fenyegetés kritikussága

C/I = Countermeasures / Ellenintézkedések

McAfee Foundstone

- Fókusz: A kritikus fenyegetéseket a fontos eszközökhöz rendelve a szervezet a leglényegesebb fenyegetésekre és eszközökre összpontosíthat, így kevesebb időt kell a biztonságra fordítania és többet foglalkozhat az elsődleges üzleti tevékenységével.
- Megfelelőség: Belső biztonsági szabványok és útmutatások kidolgozása, valamint a szabályoknak való megfelelés tanúsítása.
- Metrikák: A biztonsági döntések kommunikálására és hatékonyabb kezelésére szolgáló mérési és jelentéskészítési eszközöket biztosít.
- Műveletek: Javítja a biztonsági szintet, valamint valós biztonsági problémákat célzó műveleteket kezdeményez.

A McAfee Foundstone Vulnerability Management megoldás és a FoundScore megfelelő és körültekintő alkalmazásával a biztonsági menedzser képet kaphat az általános kockázati szintről, és ezáltal olyan döntéseket hozhat, amelyek meggátolják, hogy a fenyegetések hatással lehessenek a legkritikusabb eszközök sérülékenységeire.

A FoundScore egy olyan biztonsági kockázatosztályozó rendszer, amely az ügyfél hálózati infrastruktúrájának kulcsfontosságú aspektusait hasonlítja össze a legjobb gyakorlatokkal, azok biztonsági helyzetének számszerűsítése érdekében. A FoundScore egy intuitív 0-tól 100-ig terjedő pontozási rendszer alapján osztályozza a hálózatok biztonsági szintjének időbeni alakulását.

VII. Hetedik lépés: BLOKKOLÁS

A rendelkezésre álló új védelmi technológiáknak köszönhetően a szervezetek ma már képesek „biztonsági sérülékenységi programjavításokat” (patch) telepíteni addig is, amíg az operációs rendszer és az alkalmazások végleges javításai megfelelő tesztelésre és tervezésre nem kerülnek.

McAfee IntruShield Network Intrusion Prevention (NIPS) (hálózati behatolás-megelőzés)

Az IntruShield alkalmazásával a vállalat képes megakadályozni, hogy a legújabb fenyegetések befolyásolják hálózataikat és az azokhoz kapcsolódó eszközeiket. Az IntruShield meggátolja, hogy az önmagukat szaporító férgek kihasználják a sérülékenységeket, védelmet nyújt az ismeretlen kihasználható hibákkal (zero-day exploit-ok), az SLL-titkosítású munkafázison belüli támadásokkal, valamint az útvonal-választási (routing) vagy az átkapcsolási (switching) infrastruktúra elleni támadásokkal szemben. Az IntruShield használatával valamennyi kifelé néző hálózati szegmens és kritikus belső szegmens egy további védelmi szintet kap az ismert és ismeretlen támadások ellen.

McAfee's Secure Content Management (SCM) (biztonságos tartalom menedzsment)

Az SCM-t a levelezőszerver előtt, az úgynevezett „demilitarizált zónában” (DMZ) alkalmazva a szervezet megakadályozhatja, hogy ezeken a levelezőszervereken keresztül a végfelhasználóknak címzett rosszindulatú programok és tartalmak juthassanak be.

McAfee Enterecept Host Intrusion Prevention (HIPS) (host oldali behatolás-megelőzés)

Az Enterecept szervereken és asztali gépeken történő alkalmazása által a szervezet újabb védelmi szintet biztosíthat kritikus szerverei, notebookjai, webszerverei és adatbázis-szerverei számára. Biztosítja az üzleti folyamatok rendelkezésre állását, integritását és titkosságát a zero-day támadások, puffer-túlcsordulásos támadások (buffer overflow attack), a jogok kiterjesztése (privilege escalation) és az alkalmazás-specifikus támadások proaktív blokkolása révén. Az Enterecept viselkedési szabályokat, aláírásokat és rendszertűzfalat használ a támadások blokkolására, csökkentve ezáltal az új fenyegetéseket kezelő javítások letöltésének sürgősségét, valamint időt adva a szervezet számára a javítások kutatására, tesztelésére és alkalmazására.

McAfee VirusScan Enterprise 8.0i

Az innovatív vírusirtó technológia következő generációja.

- A rosszindulatú kódokkal és a hagyományos vírusokkal szembeni védelmen túl az Intrusion Prevention (behatolás-megelőzési) technológia puffer-túlcsordulásos támadások elleni védelmet is nyújt 23 gyakran használt Windows-alkalmazás és folyamat számára.

$$R = \frac{A}{C} \times \frac{V}{C} \times \frac{T}{C}$$

McAfee Anti-Spyware Enterprise

Az Anti-Spyware Enterprise felhasználói védve vannak a rendszerekre leselkedő legújabb fenyegetésekkel szemben, a kémprogramoktól kezdve az egyéb potenciálisan nem kívánatos programokig.

Az életciklus minden egyes lépésének alkalmazásával és az adott problémának megfelelő technológia bevetésével bármely szervezet sikeresen blokkolhatja a fenyegetéseket akár valós időben is. Azonban ha ezt nem rendszerszerűen teszik, könnyen előfordulhat, hogy bár a „megfelelő” technológiát, de a „rossz” helyre telepítik, köszönhetően a téves feltételezéseknek.

A blokkolás nem azt jelenti, hogy soha többé egy javítást sem kell letölteni, hanem hogy a szervezet képessé válik a rendszereket saját irányelvein és eljárásain belül frissíteni, ahelyett, hogy a javítást kiadó gyártó feltételei szerint tenné ezt. A végeredmény az, hogy egy „biztonsági sérülékenységi javítást” telepítenek addig is, amíg az operációs rendszer vagy az alkalmazás javítása körültekintő és ellenőrzött módon tesztelésre és alkalmazásra nem kerül. Korábban az egyetlen rendelkezésre álló lehetőség az volt, hogy azonnal ki kellett adni a javítást és reménykedni benne, hogy az nem befolyásol hátrányosan egyéb műveleteket és eszközöket.

VIII. Nyolcadik lépés: HELYREÁLLÍTÁS

A helyreállítás magában foglalja a korábbi összes lépés áttekintését, majd ezt követően a helyreállítási műveletek rangsorolását a korábbi lépések során szerzett felfedezések és műveletek alapján.

A hetedik lépés (BLOKKOLÁS) folyamatainak és technológiáinak megfelelő alkalmazásával a helyreállítási lépés megértése és végrehajtása magától értetődő lesz (bár ezt a lépést gyakran túl korán végzik el az életciklus folyamatában). A korai teljesítés – általában akkor végzik el, amikor a kritikus javítást kiadja a gyártó – eredménye gyakran az lesz, hogy nem a megfelelő technológiákat telepítik vagy csak nem a megfelelő helyre, így a javítás nem segít a támadások megállításában.

A végfelhasználó értesítése kulcsfontosságú része a helyreállítási lépésnek, célja arról gondoskodni, hogy a biztonsági irányelvek rendelkezésre álljanak. Ez lehetővé teszi a végfelhasználó számára, hogy részt vehessen a személyesen őt vagy az egész szervezetet érintő fenyegetések orvoslásában.

Fontos észben tartani, hogy nem kell minden rendszerrel, felhasználóval és adattal egyenlően bánni. Valójában a helyreállítás eredményei szükségessé tehetik, hogy az adott támadási helyzettől függően a kritikusabb rendszerek kevésbé kritikus sérülékenységeivel foglalkozzunk.

A helyreállítás sikerességét közvetlenül befolyásolja a hetedik lépésben (BLOKKOLÁS) tárgyalt, előírt védelmi technológiák alkalmazása. Ezt követően megfontolt módon lehet bevezetni a javításokat azok tesztelését követően, valamint beütemezni a helyreállítási folyamat befejezéséhez szükséges műveleteket.

McAfee Foundstone Remediation Module (helyreállítási modul)

A Remediation Module helyreállítási munkafolyamat-menedzsmentet biztosít, amely automatikusan jegyeket nyit és rendel hozzá az új sérülékenységek felfedezésekor azokhoz, illetve automatikusan ellenőrzi és lezárja azokat a javítást követően.

IX. Kilencedik lépés: MÉRÉS

Ezen lépés eléréséig már bizonyos fokú sikereket könyvelhetünk el a biztonsági rések bezárása terén. Most itt az ideje, hogy felmérjük korábbi döntéseink hatásait.

Ezen lépés végrehajtását követően azt tapasztalhatjuk, hogy korábban alkalmazott megoldásaink finomításra szorulhatnak. Bárhogy legyen is, alapvető fontosságú, hogy felmérjük korábbi lépéseinket. Továbbá ezen a ponton egy új, átfogó sérülékenységi vizsgálatot kell lefuttatni a Foundstone felhasználásával, hogy meghatározzuk a legfrissebb kockázati szintet a következő kérdések megválaszolása érdekében.

- Milyen hatással voltak a kritikus üzleti rendszerekre a korábbi lépések?
- Érte-e a rendszereket vagy a felhasználókat bármilyen negatív hatás?
- Biztonságosabb-e a környezet, mint a folyamat kezdetekor?
- Szükség van-e további lépésekre?
- Érintette-e a termelékenységet a műveletek bármelyike is? Szükséges-e ezen műveleteket korlátozni?
- Változott-e a környezet?
- Szükséges-e további technológiákat alkalmazni?

McAfee Foundstone és ePO

Mindkettő kiterjedt jelentéskészítő és mérési eszközökkel rendelkezik a folyamat során eddig, vagy a korábbi lépésekig elért eredmények szintjének meghatározására.

Mivel a Foundstone folyamatosan keresi az új rendszereket és új sérülékenységeket, a helyreállítás szintjének mérései növekvő védettségi szintet és ennek megfelelően csökkenő kockázati szintet fognak mutatni.

Az ePO-t a biztonsági irányelveknek való megfelelés ellenőrzésére és mérésére, valamint egy rendszer javítottága szintjének mérésére lehet használni a számítástechnikai környezet megfelelési ellenőrzése és mérése részeként.

X. Tizedik lépés: MEGFELELŐSÉG

Az utolsó lépés magában foglalja az egyes fenyegetési helyzetek, valamint a szervezet sikerességének kötelező vizsgálatát az adott fenyegetés kezelésében. Ez kiterjed a szervezet azon képességére, hogy felfedezze, értékelje, kezelje és helyreállítsa a biztonsággal kapcsolatos problémákat. A vizsgálat eredményei lehetővé teszik a biztonsági menedzser számára, hogy felülvizsgálja az irányelveket és meghatározza az irányelvekben és/vagy az életciklus-folyamatban elvégzendő változtatásokat, valamint hogy lépéseket tegyen a helyreállítás érdekében.

Számos tényezőt kell figyelembe venni egy ilyen jellegű megfelelési vizsgálat során, például:

- Összhangban vannak-e az eddig elvégzett lépések a biztonsági irányelvekkel?
- Szükséges-e módosítani az irányelveket az eddigi felfedezések alapján?
- A környezet vagy a felhasználói bázis szükségessé tesz-e további változtatásokat?
- Valamennyi rendszer megfelel-e a bevett szabványoknak?

Ennél a pontnál meg kell vizsgálni továbbá a számítástechnikai környezet és a felhasználói bázis új fenyegetéseit, az azokban bekövetkezett változásokat és hatásokat, az új üzleti rendszereket vagy alkalmazásokat, valamint a szervezetben történt változásokat.

A McAfee Foundstone és ePO termékeit kifejezetten erre a célra fejlesztette ki, és ezek, a kereső és megelőző termékekkel együttesen megadják a vállalat maximális nyugalomához szükséges védelmet. A megfelelés betartatása magában foglalja, hogy tudjuk, milyen eszközök vannak a hálózatban (Foundstone), ismerjük azok biztonsági szintjét (ePO), és hogy a rendszer- és hálózati hozzáféréssel kapcsolatban módosításokat végezzünk, illetve engedélyeket adjunk az előzetesen meglévő alapvető biztonsági követelmények alapján.

Összefoglalás

Naponta jelennek meg újabb fenyegetések és sérülékenységek, és hogy ezek szolgáltatói hálózatokat, vállalatokat, specifikus belső rendszereket, kritikus adatokat vagy végfelhasználókat céloznak-e, ezen a ponton lényegtelen. Az a tény, hogy léteznek, és hogy növekedésük nem lassul, arra kényszeríti a biztonsági szakembereket, hogy naprakészek legyenek nemcsak az eszközeikre leselkedő legújabb biztonsági fenyegetések, hanem ezen eszközök folytonosan változó üzleti prioritásai tekintetében is.

Annak érdekében, hogy pontosan megismerjék a kockázatokat, maximálisan meg kell ismerniük az eszközök sérülékenységeit még azelőtt, hogy bármiféle megoldást alkalmaznánk ezen eszközök tényleges védelme érdekében.

A Risk Management Lifecycle (kockázatkezelési életciklus) használata és alkalmazása révén bármely szolgáltató, üzleti vállalkozás, kormányzati ügynökség és szervezet képes lesz pontosan felfedezni, megismerni és megvédeni digitális eszközeit mind az ismert, mind pedig a „zero-day” támadásokkal szemben.