HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

INTEGRÁLT FELÜGYELETI RENDSZER

INTEGRATED MONITORING SYSTEM

PUSKÁS Béla

(ORCID: 0000-0001-6211-7579)

pb@pbnet.hu

Absztrakt

A kritikus informatikai infrastruktúrák egy összetett hálózatot alkotnak napjainkban. Emiatt is egyre fontosabbá vált alaposan megismerni és dokumentálni a rendszerelemeket, azok hatásait, kapcsolatrendszerét. Fel kell ismerni, hogy minden egyes fizikai és logikai elem hatással van egymásra, amelynek feltérképezése fontos a rendszerüzemeltetés szempontjából. Ennek egyik legfontosabb része az adatok összegyűjtése és azok rendszerezése.

Kulcsszavak: *Hálózati struktúra, Kritikus Infrastruktúra, Kritikus Információs Infrastruktúra, Szolgáltatásmenedzsment, Konfigurációmenedzsment*

Abstract

The Critical Information Infrastructures has become a complex network. Consequently, the items of the system, their mutual effects and links and the map of the network have to be known properly. We have to realize that everything is linked with each other and the physical and logical networks have mutual effects on each other as well. It is obvious, that the problem of mapping the complexity is very important. One of the most important part of the cognition is the obtainment and sorting of information.

Keywords: *Structure of networks, Critical Infrastructures, Critical Information Infrastructures, Service Management, Configuration Management*

A kézirat benyújtásának dátuma (Date of the submission): 2017.02.09.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.03.01.)

BEVEZETÉS

Neumann János 1945-ben közzétette a nevéhez fűződő Neumann-elv leírását a „First Draft of a Report on the EDVAC" művében. [1] A mai napig ezen elvek alapján épülnek fel a számítógépek, és ezen eszközök a központi részei az informatikai rendszereknek. Az elv segítségével kapcsolat épült ki az ember által betáplált adat és az elektronikus gép közt. A bevitt vagy mentett adatokon a gépben tárolt program meghatározott műveletet hajt végre, melynek eredményeképpen a kimeneten újabb adat jelenik meg, amit akár újból lementhetünk. Ez már nem csak egy célhardver, hanem egy univerzális felhasználhatóságot elősegítő szerkezeté vált. Kezdetben önálló és egyszerű felépítésű szerkezet volt, mára azonban világméretű hálózat épült ki a gépekből, amelynek a koordinálása szinte lehetetlen. Neumann már 1948-ban a Hixon Symposiumon tartott előadásában feltette a kérdést, amely a mai napig komoly kihívást okoz az informatikai rendszereket tervezését és üzemeltetetését végző személyek számára.

AZ INTEGRÁLT FELÜGYELETI RENDSZER

„Lehet-e megbízhatatlan szerkezeti elemekből megbízhatóan működő automatákat építeni?" [2, 50. o.]

A Hixon Symposiumon tartott előadások leginkább a számítógépek megbízhatóságával foglalkoztak, de ma már az összetettebb rendszerekkel kapcsolatban még inkább felmerülő kérdésé vált. A számítógépeket felépítő elektronikai alkatrészek nem örök életűek és bár statisztikai adatok rendelkezésünkre állnak, de azt, hogy mikor melyik alkatrész fog meghibásodni nem tudhatjuk. A hibamentes működést elősegíthetjük az ideális közeli környezet kialakításával, a rendszer *„hibatűrő"* kialakításával, a folyamatok szabályzásával, stb. Azt szokták vizsgálni, hogy egy rendszerelem meghibásodása milyen hatással van a rendszer egészének működésére. Azonban ez egy kezdetleges számítógép esetében sem volt egyszerű nemhogy egy adatközpont, vagy összekapcsolt adatközpontok esetében. Egy váratlan vagy nem kívánt esemény hatásának csökkentése az ugyanolyan feladatot végző rendszerelemek párhuzamos üzemeltetésével, különböző technológiák, gyártók bevonásával, de független energia-szolgáltatókkal, telekommunikációs cégekkel történő szerződéssel is elősegíthető. Természetesen a költségek és az adminisztrációs többletfeladatok miatt mérlegelni kell mikor éri meg ez. Hibás működésből adódó becsült veszteség és a befektetett költségnek összhangban kell lenni. A rendszerünknek robusztusnak és alkalmazkodónak kell lennie, csillapítva ezáltal a nem kívánt hatásokat. Ez azt jelenti, hogy a hibákat részben elnyeli vagy késlelteti azok kimenet hatását. Diverznek tekinthető a rendszerünk, ha a rendszerelemeket, bemeneti forrásokat, technológiákat párhuzamosan alkalmazzuk.

A természetben megfigyelhető jelenségeket, mint az öngyógyítást több dolog miatt is nehéz megvalósítani egy ember által épített és kézben tartott rendszernél. Egyrészt olyan mértékű túlbiztosításra és kapcsolati rendszerre lenne szükség, amely már túlzott mértékben megdrágítaná a rendszerünket, másrészt pedig folyamatos kontroll alatt akarjuk tartani a rendszerünket (legalábbis ma még ez a cél) és nem engedhetjük saját életet élni, ill. ma még nincs is rá módunk. Véleményem szerint ma egyre inkább fontosabb Neumann megállapítása, amely azt mondja:

„… valamely szerkezet működési biztonságát nemcsak technikai eszközökkel, hanem lényegében véve szervezési eszközökkel is növelni lehet." [1]

[1] Idézet: Neumann János: A számológép és az agy. [2]

A szervezési és irányítási eszközöket segíti, ha a vállalatnál létrehozunk egy konfigurációkezelő rendszert. Az angol elnevezése többet mond, mint a magyar fordítás, így a továbbiakban az eredeti angol elnevezést CMS (Configuration Management System) használom. Az ITIL3[2] megfogalmazás szerint a CMS egy szoftver, amely képes kezelni az informatikai szolgáltatásokat biztosító összetevők és a köztük lévő kapcsolatok konfigurációját. Magába foglalja továbbá az incidenskezelést, problémamenedzsment, tudásmenedzsment, változáskövetést, erőforrás-kezelést és dokumentumkezelést, valamint ezek kapcsolatrendszerének kezelését. Az alapadatok szintén tartalmazzák a rendszerrel kapcsolatba kerülő személyek, helyszínek, erőforrások, üzleti folyamatok és a környezet leírását. Azonban a CMS nem egyenlő a CMDB[3]-vel.

A CMDB naprakészségéért a konfigurációmenedzser a felelős, aki a konfigurációmenedzsmenten keresztül, azok irányításával hajtja végre a feladatot. Egy jó CMDB-ét azonban az IT rendszert üzemeltető valamennyi személy, szolgáltatásmenedzsment használja. Két dolog miatt is fontos ez. Egyrészt ha mindenki ezt használja, akkor nem fognak kialakulni szigeteket alkotó önálló adatbázisok, nyilvántartások, amelyek átfedéseket, eltérések tartalmazhatnak az üzemeltető egységek közt. A másik fontos szempont, hogy az adatbázist mindenkinek magának kell éreznie, mert csak így biztosítható, hogy a személyzet folyamatosan karbantartsa az adatbázist, aminek ez a naprakészség legkritikusabb pontja. Amennyiben elhanyagolják a folyamatos adatkarbantartást az adatbázis rövid időn belül használhatatlanná válik. Minden szereplőnek úgy kell érezni, hogy az adatbázis az ő érdekeit szolgálja, ezért érdemesnek, sőt kifejezetten hasznosnak érzik azt karbantartani. Olyan megjelenítő felületeket kell alkalmazni, amelyek az egyes szinteknek megfelelő, a számára leglogikusabb és hasznosabb információkat közöl. Ösztönzőleg hathat, ha a felső vezetők is kapnak összefoglaló információkat, így ezek elmaradása, a téves adatok kérdéseket szülhetnek. Ahogyan a CMS nem egyelő a CMDB-vel, úgy a CMS sem egyenlő a feltérképező szoftverek által biztosított adatokkal. Az csak egy kisegítő eszköz, amely leginkább az auditálásra szolgál. Hasonlóan nem keverhető össze a hálózatfelügyeleti és rendszerfelügyeleti eszközök, szoftverek által szolgáltatott adatok nyilvántartása, tárolása. Ezek az alrendszerek a CMS rendszer részét kell, hogy képezzék, de nem válthatják ki egymást. Fontosnak tartom, hogy a CMDB magját azok az adatok alkossák, amelyek a jóváhagyási mechanizmus után kerülnek be. Ebből következik, hogy a rendszer részét kell képezze egy munkafolyamat leírás, amelyet a szolgáltatást biztosító személyek mindegyikének be kell tartani. A rendszerbe kerülő elemek adatait az egész életútjuk alatt nyilván kell tartani. A változásoknál a régi adatokat nem szabad törölni, azokat archiválni kell a későbbi kereshetőség érdekében.

Nagyon érdekes kérdés és problémakör, hogy egy rendszerelem (ITIL-ben konfigurációs elem[4]) mennyi tulajdonságát kell rögzíteni. Természetesen ennek meghatározása a rendszer kialakításakor kell, hogy megtörténjen. A mélységében és szélességében is vizsgálható a kérdés. Mélység alatt értem, hogy mennyire kell részleteiben vizsgálni egy eszközt. Például kell-e, tud-e hosszútávon információt adni egy Routerben lévő kondenzátor, tekercs típusa, gyártmánya, stb. Kell-e nekünk az őrzésvédelmi rendszereket alkotó kameráit gyártó cég tulajdonosi szerkezetét vizsgálni?

[2] ITIL (IT Infrastructure Library): Az IT-szolgáltatásmenedzsment számára jól bevált gyakorlatot leíró útmutatók gyűjteménye. Az ITIL tulajdonosa az OGC, és olyan kiadványok sorozata, amely minőségi IT-szolgáltatások nyújtására ad útmutatást, valamint a támogatásukhoz szükséges folyamatokra, és létesítményekre. További információért ld. http://www.itil.co.uk/. [5]

[3] CMDB: Konfiguráció Management Adatbázis

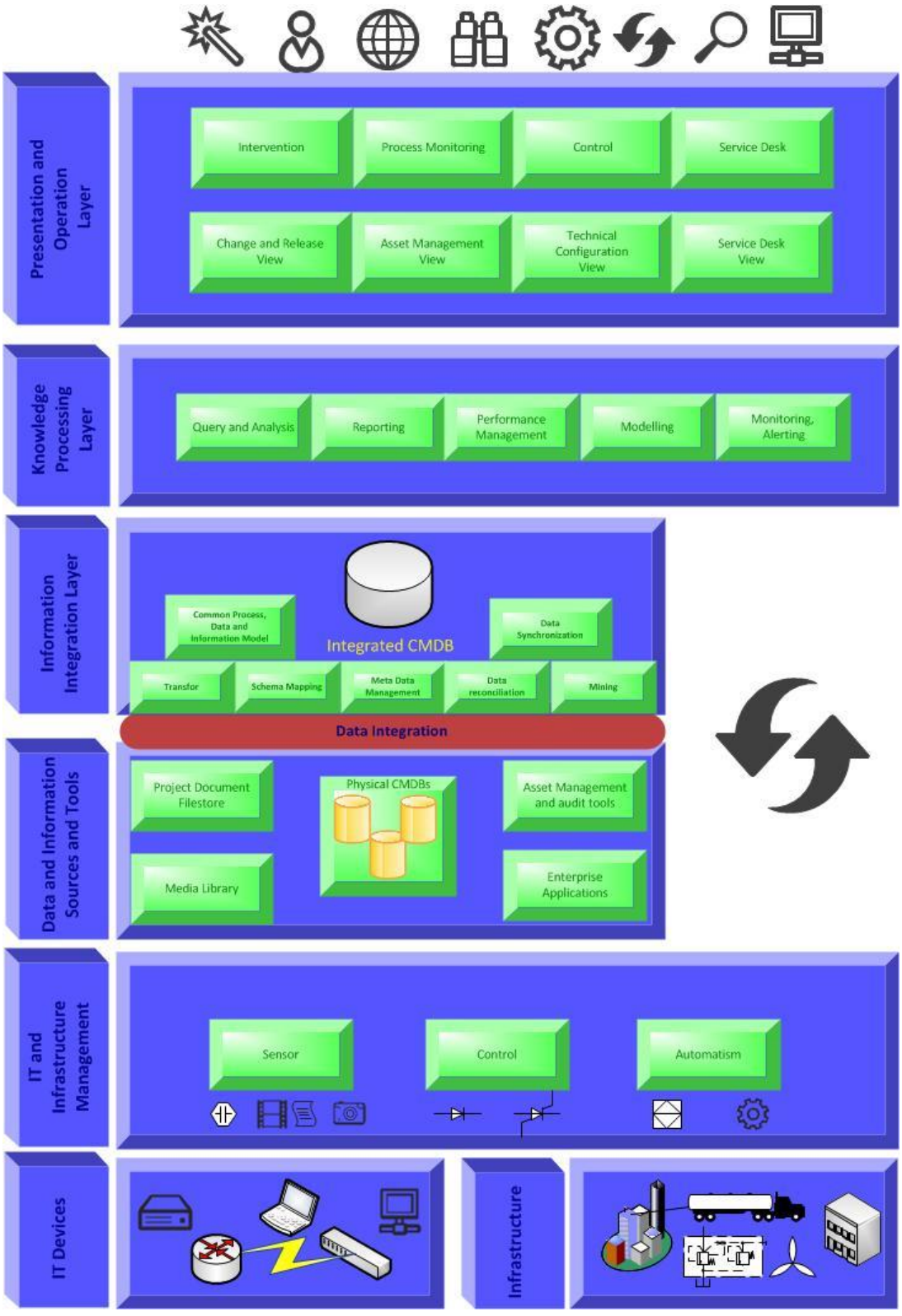
[4] Bármelyik komponens, amelyiket felügyelni kell valamilyen IT-szolgáltatás nyújtása érdekében.

Ezer ilyen kérdést tehetünk fel, amelyek elsőre talán meghökkentő és talán nevetséges is, de egy kiemelten védett infrastruktúrák esetében már lehetnek érdekes részei is. Természetesen mindig kérdés, hol alkalmazzuk a CMS rendszerünket. Egy vegyipari cégnél elképzelhető, hogy sok olyan paraméter érdekes, amely egy katonai, nemzetbiztonsági cégnél nem, és fordítva is igaz. Ezeket az adatokat a kockázatelemzésnél is fel kell használni. Érdekes azonban, hogy pont a kockázatelemzésből derülhet ki, hogy milyen adatokat kell nyilvántartanunk még. A szélesség alatt pedig azt értem, hogy milyen messze nyúl el a nyilvántartás keze. Amennyiben meghatározzuk, hogy a cégen belül egy bizonyos szegmensig tartok mindent nyilván, akkor azon belül minden egyes elemet el kell érnünk az adatszolgáltatás szintjén. Hasonlóan, hogy ha a kapcsolódó cégek adataira is szükség van, akkor az összes beszállító cégnél meg kell követelni az adatszolgáltatást. Tehát biztosítani kell az egyenszilárdságot, annak érdekében, hogy használható elemzéseket tudjunk elkészíteni.

Minél nagyobb és „kritikusabb”[5] egy informatikai infrastruktúra annál bonyolultabb, összetettebb felépítésű és annál nehezebb az üzemeltetés számára egy CMS segítsége nélkül átlátni az egész működését. A rendszerelemek bonyolult kapcsolatai eredményezhetnek olyan nem várt esemény bekövetkezését, amely negatív irányba mozdíthatja el a rendszer működését.

Kiegészítve az ITIL ajánlását az **1. ábra** segítségével mutatom be a CMS kialakítását.

[5] Kritikusabb alatt azt értem, hogy az üzemszerű és elvárt működéstől való eltérés veszélyeztethet más rendszerek, emberek, közösségek életminőségét negatív irányba.



1. ábra CMS felépítése (a szerző szerkesztése a [6] alapján)

Az ábrán látható mitől több a CMDB-nél egy CMS felépítése.

A legalsó szinten helyezkednek el az IT és a hozzátartozó (épület elektronikus berendezései, klíma, UPS, beléptető és riasztó rendszer, tűzérzékelő és oltórendszer, zártláncú videó hálózat, stb.) infrastruktúra elemek.

Ez a szint minden esetben megvalósul, még ha hiányosan is, mert különben nem is létezne informatikai rendszer.

A következő szinten az érzékelők helyezkednek el. Ezek általában rendszerenként a gyártó által szállított szoftverrel van ellátva. Itt találhatóak meg a rendszereket - általában a gyártó által szállított - vezérlő eszközök, szoftverek. Léteznek integrált rendszerek is, ilyenek például azok a biztonsági rendszerek, amelyek egy egységet képeznek a beépített beléptető, riasztó, zártláncú videó és tűz jelző rendszerek által. Ezek kimenete sokszor az IT rendszer bemenete is lehet, amikor például a tűz, vízbetörés esetén utasítják az IT infrastruktúrát a rendszer mentésére, leállítására. Ezen a szinten már információs infrastruktúráról beszélünk, mert az infrastrukturális elemeket komplexen kezeljük.

A következő szinten jelenek meg a rendszerenként különálló CMDB-k, vagy a dokumentum könyvtárak. A szenzorokból érkező jeleket átalakítást követően az adatbázisban tároljuk. Itt nagy a felelőssége az adatbázis tervezőnek, mert nem adatokra, hanem információkra van szükségünk. Ezt azonban sokszor a nagyon sok adatból nem lehet kihámozni, a nagyon kevés adat pedig téves információkat adhat.

Az integrációs szinten jelenik meg az egységes CMDB. Ez lehet valóban egy önálló adatbázis, de hasznosabb, ha virtuális értelemben jelenik meg csak egy adatbázisban. Ahhoz, hogy a különböző adatbázis adatait egységként kezeljük szükséges például az adatok meta adatait központilag kezelni, elvégezni a szükséges átalakításokat, a közös pontokat megtalálni és nyilvántartani. Természetesen a szinkronizáció ütemezése és végrehajtása az egyik legkomolyabb feladat ezen a szinten.

Amennyiben rendelkezésünkre áll a tömeges adat, akkor a tudásbázis szinten kezelhetjük azokat. Itt nem csak az aktuális adatokat, de az archiváltokat is hasznosítani lehet, illetve kell. Itt valósulnak meg a különböző elemzések, lekérdezések, a modellalkotások, amelyek segítségével algoritmusokat hozhatunk létre. Az adatok halmaza, azok kapcsolódása, időbeni változása olyan összefüggéseket mutathat, amelyet külön-külön nem vehetnénk észre. A rendszer riasztási eseményeit összetetten lehet kezelni, amely hatékonyabb beavatkozáshoz vezethet.

A legfelső rész gyakorlatilag a rendszerfelügyeleti szint, a jelzéseket, elemzéseket megtekinthetjük, utasításokat adhat ki az üzemeltető személyzet. Ez a szint biztosítja a felső vezetés részére is az információ megjelenítést. A tudásbázis által biztosított algoritmusok és az adatbázis adatai segítségével automatizmusok által javaslatokat tehet a felügyeleti rendszer a beavatkozásra, vagy akár automatikusan végre is hajthatja azokat.

Abban az esetben, ha külső információáramlás is szükséges, akkor ellenőrzött formában becsatlakozhat különböző szinteken is az együttműködő szervezet. A maximális biztonságot is szem előtt tartva a kapcsolat egyirányú kell, hogy legyen, és a kimenő adat az ellenőrzést követően adatdióda segítségével továbbítható.

A CMS kiépítettségét tekintve egy cég különböző fejlettségi szinten lehet. Legtöbb esetben sajnos a harmadik és a negyedik szinten vannak a cégek. A kiépítést a moduláris felépítés miatt lehetőség van szakaszosan végrehajtani. Az egyik legkritikusabb rész egy már működő cég esetében az adatbázisok integrációja, a közös CMDB létrehozása. A CMDB-t tekintve is több fejlettségi mutató lehet, amelyek a következők:

- Az információk a rendszerről többnyire a közvetlen üzemeltető állomány fejében létezik. Legtöbbször a tudás hatalom elv alapján nem osztják meg az információt mással, így vélik biztosítottnak a munkahely megmaradását, a nélkülözhetetlenséget;
- Valaki leírja saját Word, Excel dokumentumba, jobb esetben valamilyen adatbázisba a saját számítógépén. Egy bonyolultabb rendszernél már nem valósítható meg, mert az hamar a rendszer összeomlásához vezetne;

- Az előbb létrehozott nyilvántartásokat a közös mappákban tárolják. Ebben az esetben, ha az üzemeltető személlyel történik valami, van esély a leírás megtalálására;
- Ezen a szinten már a közös mappában tárolást valamilyen szabály írja elő, így a mapparendszer is előre kidolgozott, átlátható. Így valóban kezelhető az információ abban az esetben is, amennyiben kiesik a rendszert alkotó személy, személyek;
- Egy magasabb fejlettség, amikor már adatbázisban tárolják az adatokat. Így az adatok gyorsan kezelhetők, azokkal könnyebb feladatokat végrehajtani;
- A következő szint, amikkor az összes információ egy fizikai vagy virtuális adatbázisban tarolunk, amely természetesen szabályozott módon történik;
- A legfejlettebb, amikor a cég normál működése során már nem is lehet végigvinni egy folyamatot a CMDB használata nélkül;

Véleményem szerint egy kritikus információs infrastruktúrát üzemeltető cégnél szükséges a legmagasabb szintet elérni. Ezek a rendszerek már annyira bonyolultak, hogy másképpen nem kézben tartható a biztonságos üzemeltetés. A másik fontos szempont, hogy a kezelő személyektől nem függhet közvetlenül az infrastruktúra működése. A személyzet cserélődése nem okozhat fennakadást. Az információ minden esetben rendelkezésre kell, hogy álljon az új szakembereknek is a lehető legrövidebb időn belül. Persze nagyon nehezen helyettesíthető az a karbantartó munkás, aki az iskola elvégzését követően már a cégnél dolgozik és készül nyugdíjba menni, de egyszer mindenki elmegy a cégtől. Amennyiben a cég rendelkezik a legfelső szinttel logikus felépítéssel, „szervezési" eszközökkel viszonylag könnyen megvalósítható a CSM rendszer passzív állapota[6]. A szintek egyes funkciói nem minden esetben valósulnak meg egy időben. A legfontosabb a közös adatbázis, amin a tudásbázis elemek folyamatosan bővíthetők. A közös kezelőfelületbe folyamatosan integrálhatók a gyártók által szállított kezelőfelületek. Persze itt is van egy nagy kérdés. A gyártók rendelkezésre bocsájtanak-e minden információt, biztosítják-e a megfelelő csatolófelületet az információáramláshoz. Üzemeltetés szempontjából nagy előnyt jelenthet egy homogén rendszer kialakítása, azonos gyártók kiválasztása. Ez azonban ellentmondásban van azzal, hogy a magas rendelkezésre állás különböző technológiák, gyártók alkalmazását követeli meg.

Eddig még nem eset szó az egyik legfontosabb rendszerelemről, az emberről, amelyről jelenleg a CMS rendszerek nagyon kevés információt tárolnak. Ráadásul ezeket az adatokat teljesen más módszerrel kell felvinni a CMDB-be, mint a rendserek adatait.

Mik is lehetnek ezek az adatok? Fontos kérdés a személyzet, felhasználók képzettsége, tapasztalata és egy sor jellemzője, amely befolyásolja a rendszer működését. Ilyen például a viselkedés, melynek rögzítésére már ma is rengeteg eszköz áll a rendelkezésünkre, de léteznek olyanok is, amelyek a személy együttműködése nélkül is összegyűjthető, ilyen a viselkedés alapú profilkészítés. Persze ezek sok erkölcsi és jogi kérdést is felvetnek, de létezhet olyan hely, ahol ezzel együtt kell élni. A hétköznapokban is megfigyelnek ilyen eszközökkel minket, amikor az Internetet használjuk, majd ezeket az adatokat kereskedelmi céllal fel is használják. Lépten-nyomon otthagyjuk a digitális nyomunkat mindenhol, ahol az informatikai eszközök által kezelt rendszereket használjuk.

[6] Passzív alatt azt értem, hogy a rendszer nem képes automatikusan beavatkozni a működésébe. A kezelőszemélyzet egy rendszert használ, jogosultsági szintnek megfelelő lekérdezéseket tudnak végrehajtani és utasításokkal vezérlik a rendszert.

Ilyenkor nem csak az internet (e-mail, közösségi média, weblapok, internetes csevegő- és telefonszolgáltatások, stb.), de a mobiltelefon, a GPS eszköz, bankkártya, banki szolgáltatás használat, térfigyelők felvételei és még számos tevékenységünk digitális lenyomata ott marad valahol. A banki adatbázisból kiderülhet, hol vásárolunk, mikor és mennyiért, kinek milyen rendszerességgel utalunk pénzt, vagy ki utal nekünk, ezáltal megtudható, kikkel vagyunk kapcsolatban. A mobiltelefonunk aktív használat nélkül is folyamatosan árulkodik a hollétünkről, hová milyen gyakorisággal megyünk és ott mennyi időt töltünk. Érdekes adat az Internet használatakor, hol mennyit időztünk, milyen billentyűzet vagy egér aktivitásunk van, honnan jöttünk és merre tartunk. Talán mégis a legveszélyesebbek a felhőben tárolt adatok. Sajnos sok cég az ügyfelek adatait tárolja üzletileg egyes esetekben talán valóban a leghatékonyabb egy harmadik fel által biztosított szolgáltatásként a virtuális IT környezetben. De ezeket az adatbázisokat összekötve egy cég biztonsági rendszerével, mozgásnaplónkkal és kapcsolati hálónkkal még értékesebb információt kapunk. Főleg, ha nem csak az aktuális adatokat figyeljük, hanem tendenciákat és összefüggéseket keresünk.

Mint mindent ezt is lehet jó és rossz dologra felhasználni, de egy biztos, hogy ezek a technológiák léteznek és használják már őket. A kérdés, hogy mikor kapcsoljuk ezeket mind össze, illetve mikor leszünk képesek kezelni az óriási mennyiségű adatot. Véleményem szerint nem a biztonsági terület lesz, az ahol esőként hasznosítják az elméletben elért eredményeket. Az üzleti élet gazdasági szereplői a potenciális vásárlók felkutatásánál és a reklámok célba juttatására hatékony módszer lehet, így rengeteg pénzt fordítanak rá, és az emberekkel is elfogadtatják a kellemetlen oldalát is. [3] Az emberek viselkedésének az elemzéséhez jól jöhet a környezeti hatások adatbázisba mentése. Ugyanis az embereknek az a normális viselkedése, hogy követni akarják a társadalmi normákat, a csoportok viselkedését, és a legtöbben feljebb és feljebb akarnak kerülni, vagy meg akarnak felelni a cégüknek, főnöküknek. Ezekből a viselkedési formáktól a környezeti változás fogja őket eltéríteni. A rendszerünk viselkedésének megjóslásánál az emberi tényezők mellett, amelyek sokszor kiszámíthatatlanok, a gyártók megadnak az alkatrészek, eszközök tekintetében olyan adatokat, amely a meghibásodási valószínűséget mutatják. Ezeket az adatokat is bevihetjük az adatbázisunkba, így a gráfelméletben alkalmazott algoritmusok segítségével olyan elemzéseket végezhetünk, amik a rendszer nagyobb megbízhatóságát segítik elő.

Természetesen az adatok gyűjtésével és elemzésével a gazdasági élet szereplői mellett már ma is foglalkoznak a rendvédelmi szervek és titkosszolgálatok. Sajnos a kapcsolódások bonyolultsága és az adatok számossága nem segíti elő a robbanásszerű fejlődést, de talán a hálózatkutatásban elért eredmények segíthetnek ezen. Egy ilyen a nemrég megjelent publikálás is, amely Babai László matematikus nevéhez kötődik, aki jelenleg a Chicagói Egyetem oktatója. Ő egy új eljárást mutatott be, ahol egy algoritmus segítségével gyorsabban megállapítható, hogy két gráf azonos-e. Ez segítséget nyújthat az informatikai rendszerek felügyeleténél, persze akkor, ha megfelelő számú információ áll a rendelkezésünkre. [4] Hasznos lehet például, ha a mintákat, az előzményeket összehasonlíthatjuk az aktuális helyzettel. A módszer tűzfalak esetében már ma is egy létező gyakorlati alkalmazás, de az összetett rendszerek esetében még nem.

A fejlődést szintén nagyban felgyorsítja Barabási Albert-László kutatásai, aki a hálózatelméleti kutatásai során informatikai rendszerek felépítéséből, vagy éppen a telefontársaságok által átadott névtelen adatbázisokból alkot olyan megállapításokat, amelyek a hálózatok egészére vagy legalábbis tipikus hálózati felépítésre igaz.

A CMS használatához, mint az időjárás előrejelzés esetében is sok adatra van szükség, és minél későbbi bekövetkezendő eseményt akarunk előre jelezni, a megbízhatósága annál bizonytalanabb lesz. Egy nem várt eseménynél a reagáláshoz az üzemeltető személyzetnek a lehető legtöbb időre van szüksége, hogy biztosítsa az üzletmenet folytonosságot az informatikai rendszerek segítségével.

Sajnos azonban ma a legtöbb védelmi és a riasztást kiváltó eszköz már csak az esemény bekövetkezésekor jelez, amikor azonnal reagálni kell. Értékes információ lehet a kezelőszemélyzetnek az is, hogy mi és mikor várható a rendszerünkben, ha például leáll egy rendszer eleme, vírussal fertőződik meg, kiesik egy összeköttetés. Ezeket sok adat elemzésével a CMS tudja biztosítani.

Neumann megállapítása, amikor a szervezési eszközöket említi mindenképpen igaz a kritikus információs infrastruktúra esetében is. Azt, hogy a szűk reagálási időt hogy hogyan használjuk ki, az előre megtervezett intézkedési stratégiákkal lehet a leghatékonyabbá tenni, és egy komplex rendszerre kidolgozott biztonsági, üzemeltetési utasítással, rendszabállyal lehet a bekövetkezés előtt megnövelni a várható időkeretünket. A CMS pedig elősegíti az átláthatóságot és egyes esetekben az automatizmussal csökkenti a reagálási idő is. Úgy működik, mint a Neumann elv a tárolt adatokon az előre megírt (vagy a folyamatában kidolgozott) program elvégez műveleteket. A cél a stabil állapot fenntartása.

KÖVETKEZTETÉSEK

Egy rendszer nem csak az eszközöktől válik biztonságossá. A jól megtervezett rendszer tartalmazza a szükséges eszközöket és a rendszer üzemeltetéséhez és használatához szükséges rendszabályokat. Már a rendszer fejlesztése során a tervezési fázisban gondoskodni kell a megfelelő szabályozottságról. Azonban nagyon fontos, hogy nem a jogszabályok és ajánlások betű szerinti betartása a fontos, ennél több kell, a szellemiséget kell átvenni és alkalmazni.

Hasonlóan, ahogyan ma mára tűzfalak is „tanulnak” a szokásainkból, az elmúlt időszak eseményeit elemzik, így a CMS rendszereken keresztül a kritikus információs infrastruktúráknál is egyre inkább alkalmazni kell ezt a módszert. Az eseményekhez hozzárendelve annak bekövetkezésének idejét az idő múlásával a felgyülemlett adatokból egyre megbízhatóbb és több jóslást adhat a rendszerünk az esetleges nem várt események bekövetkezésére.

A Neumann János állítása miszerint valamely szerkezet működési biztonságát nemcsak technikai eszközökkel, hanem lényegében véve szervezési eszközökkel is növelni lehet ebben az esetben is igazolható. Egy rendszernek minél kisebb az entrópiája[7], az annál rendezettebb, tehát a 0 entrópiájú rendszerhez kell közelítenünk ahhoz, hogy minél inkább kézben tarthassuk a rendszerünk irányítását. Ehhez azonban ismernünk kell a rendszerünk elemeit, kapcsolódási pontjait és természetesen ezek egy gondosan megtervezett folyamatosan kontrolált fejlesztésen, majd üzemeltetésen kell átesniük.

FELHASZNÁLT IRODALOM

[1] NEUMANN, J. V.: First Draft of a Report on the EDVAC, Pennsylvania: University of Pennsylvania, 1945.

[2] NEUMANN J.: A számológép és az agy, Budapest: Gondolat Könyvkiadó, 1964.

[3] ALBERT-LÁSZLÓ, B: Kiszámítható-e az emberi viselkedés dinamikája? www.ceeol.com Megtekintés ideje: 2015.11.26

[7] *„Az entrópia azt mutatja meg, hogy mennyire rendezett egy rendszer belső viselkedése. Minél nagyobb a rendszer entrópiája, annál rendezetlenebb. Az entrópia tehát a rend mértéke. Azért fontos, mert szorosan össze-függ a jósolhatósággal.”* [3]

[4] CHO, A.: Sciencemag.org http://news.sciencemag.org/math/2015/11/mathematician-claims-breakthrough-complexity-theory Megtekintés ideje:2015.11.18

[5] itSMF Hungary: ITIL® Glossary of Terms, Definitions and Acronyms in Hungarian, V3.1.24.h2.5, Budapest: itSMF Hungary, 2008.