ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel

Információbiztonsági program

Molnár Bálint

Nemzeti Közszolgálati Egyetem

Budapest, 2014

TARTALOMJEGYZÉK

ÁBRAJEGYZÉK

TÁBLÁZAT JEGYZÉK

DEFINÍCIÓ JEGYZÉK

1 BEVEZETÉS

E fejezet tárgya ***informatikai biztonsági program*** kifejlesztésének és kezelésének áttekintése. Ez az oktatási anyag a közigazgatásban dolgozó *informatikai biztonsági vezetők* számára készült. Egy sikeres informatikai biztonsági program kialakításához és megvalósításához három lényeges elemre van szükség:

- A programnak magának egy jól kidolgozott informatikai biztonsági stratégiára kell alapulnia., amely a szervezet célkítűzéseit támogatja.
- Az informatikai biztonsági programot a (felső) vezetéssel és az érdekelt felekkel együttműködve kell kidolgozni.
- Olyan eredményes mutatószámrendszert, indikátorokat, metrikát kell létrehozni, hogy az informatikai biztonsági program kifejlesztésének és megvalósításának eredményességé és sikerességét tényelgesen mérni lehessen, és e mérőszámok alapján pozítiv visszacsatolást lehessen adni az elért eredményekről a program kialakítói és vezetés felé.

Ebben a fejezetben felvázoljuk azokat a módszerekt is, amelyek segítenek a kívánt biztonsági állapot megfogalmazásában és egy átfogó program kifejlesztése révén ezen célok és célkitűzések elérésében.

Az informatikai program létrehozásának fő célja az *informatikai biztonsági stratégia* megvalósítása tekintet nélkül arra, hogy vajon az informatikai biztonsági célokat, milyen módon fogalmazták meg.

Az *informatikai biztonsági program* kialakítása akkor sikeres, ha a szervezet által alkalmazott igazgatási, szakmai terminológiájában, fogalmai segítségével írták le, ennek révén a nem műszaki, informatikai képzettségű érdekelt felek is meg tudják érteni és támogatni tufják a program célkítűzéseit.

2 JOGI ÉS SZABÁLYOZÁSI HÁTTÉR

Az *elektronikus információs rendszerek* és az *információrendszerek* használatának mindennapivá válása mind a közigazgatásban mind általában a gazdasági, társadalmi életben szükségessé tette az információbiztonság törvényi szabályozását. Az elektronikus információs rendszerek világának, az Internetnek, a *kibertérnek* egyik sajátossága, hogy *teremtett világ*, de ez az ember által teremtett világ egyre inkább befolyásolja a valóságos világot és gazdasági és egyéb hatásokat is kifejt.

A fejlett ipari államok, amelyek intenzíven és extenzíven alkalmazzák információtechnológiát már több mint két évtizeddel ezelőtt megkezdték a törvényi szabályozást. A 9/11 (2001-09-11), a STUXNET (az iráni urándúsító elleni vírus támadás), a kreatív könyvelés révén végrehajtott gazdasági bűncselekmények (ENRON stb.), majd a számítási felhő és az Interneten keresztül a szoftver és informatikai alkalmazási rendszer szolgáltatások egyre szélesebb körű használatával kapcsolatban fellépő információ kezeléssel összefüggő botrányok (PRISM) nemzeti és nemzetközi szabályozások iránti igényt teremtettek. A *kibertér védelme* elsősorban az Amerikai Egyesült Államokban jelent meg, de a 2007-es Észtországi kiber támadások (vélhetőleg orosz felek részéről), majd állítólagosan kínai „amatőr informatikai betörők" (hackerek) támadásai illetve támadási kísérletei egyes USA kibertérbeli objektumai ellen mutatnak olyan példákat, amelyek szélesebb körben is értelmezhetővé teszik a fogalmat, illetve a szükséges óvintézkedések kialakítását.

Az Európa Unióban is elindult egy általános jogi iránymutatás és stratégia kialakítása szintjén egy szabályozási folyamat[1]. Ezt követte nyomon a magyar szabályozás is a „**Magyarország Nemzeti Kiberbiztonsági Stratégiája"**[2] formájában**.**

Az elektronikus információbiztonságról szóló törvény és kapcsolódó végrehajtási rendeletek kodifikálása, hatályba léptetése és tényleges megvalósítás 2013-2014 folyamán történik történt.

2.1 Kibertér, elektronikus virtuális valóság és Internet

A **kibertérnek** nincs szabványos, szabatos definiciója, eltérően más informatikai és információtechnológiai fogalmaktól. A kibertér fogalmát a számítógépek virtuális világára használják. A kibertér egy *objektuma* általában adatok egy halmazát jelenti, amely a számítógép rendszerek és számítógép hálózatok között áramlik. Az Internet kifejlődésével a kibertér fogalma kiterjedt a számítógépek világot átfogó, globális hálózatára. Ebben a környezetben, ha egy e-

mailt valaki elküld a barátjának, azt mondhatja, hogy a saját kiberterén keresztül küldött egy üzenetet az ismerősének.

Kibertér

- globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek összessége, továbbá az *elektronikus rendszerekhez* szorosan kapcsolódva, e rendszereken keresztül *adatok* és *információk* formájában megjelenő, szervezeti, közigazgatási, vállalati, társadalmi és gazdasági *folyamatok* együttesét jelenti..

> *A **kibertér** szót (kibernetika + tér) William Gibson tudományos-fantasztikus (sci-fi) szerző alkotta meg 1982-ben megjelent "Burning Chrome" című novellájában és 1984-es Neurománc című regényében. Gibson definíciója : << a **kibertér** konszezuson alapuló tömeges hallucináció, amelyet a tényleges használók milliárdjai tapasztalanak meg minden nap, minden országban és minden nemzetben, pl. azon keresztül ahogy a gyermekeknek matematikai fogalmakat oktatnak. A **kibertér** egy olyan absztrakció, amely az emberekből álló és általuk alkotott rendszerekben létező számítógépek sokaságából származtatott adatok alapján egy komplex diagramban ragadható meg. Elképzelhetetlenül bonyolult. Az emberi elme nem térbeli tartományában fény sugarak terjednek, adat klasztereket és együttállásokat teremtve.>>*
>
> *„The word "cyberspace" is credited to William Gibson, who used it in his book, Neuromancer, written in 1984. Gibson defines cyberspace as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data" (New York: Berkley Publishing Group, 1989), pp. 128."*

A társadalmi és gazdasági folyamatok egyre nagyobb hányada zajlik az Interneten keresztül, ez a jelenség, ennek a „virtuális világnak” a kialakulása hozta létre a *kibertér* fogalmát. A *kibertér* létező valóság, amelyben globálisan több milliárd ember – Magyarországon mintegy három millió – , felhasználó jelenik meg. Ebben a térben az egyének társadalmi életet élnek, csoportok és pártok szerveződnek, a gazdasági élet szereplői pedig szolgáltatásokat nyújtanak, pénzt és árukat mozgatnak.

A *kibertér* egyben az a szféra, ahol az államok egyre gyakrabban érvényesítik *nemzetbiztonsági*, illetve *nemzetgazdasági* érdekeiket védekező vagy támadó jelleggel a kibertér nyújtotta lehetőségek felhasználásával. A kibertér nincs tekintettel az állami határokra, eszközeit és infrastruktúráját meghatározó mértékben az *üzleti szektor szereplői* birtokolják, üzemeltetik és felügyelik. További jellegzetessége a kibertérnek, hogy a nincs irányító központja, új elektronikus információs rendszerekkel (mint például a **mobil internet** vagy az **számitási felhő** (*Cloud Computing*)) naponta bővül és *állami eszközökkel* csekély mértékben szabályozható.

Magyarország *kibertere* a Magyarországon található, a globális *kibertér* részét képező elektronikus információs rendszerekből és ezeken az elektronikus rendszereken keresztül *adatok* és *információk* formájában *megtestesülő*, Magyarországra irányuló, és hazánkban megjelenő társadalmi és gazdasági folyamatok összességéből áll.

A *decentralizált*, gyorsan növekvő, államilag nem szabályozott kibertér egyre *nagyobb* biztonsági problémákat vet fel, ebben a környezetben a *névtelenség* és a követhetetlenség mögé bújva a következmény-nélküliségben remélve lehet hírszerző tevékenységet folytatni, kormányzati és üzleti rendszerek adatait megszerezni, nyilvánosságra hozni, mások tulajdonát törvénytelen eszközökkel elvenni. A kibertérből jövő támadások eredetét igen nehéz egyértelműen megállapítani, leginkább a *kibertámadások* céljából, eszközrendszeréből és nagyságrendjéből lehet következtetni arra, hogy hagyományos *kiberbűnözés* vagy államilag finanszírozott támadás ellen kell védekezni. Fentiek alapján a kibertérben megjelenő veszélyek forrásuk szerint az alábbi nagy csoportba oszthatók: *állami* vagy *üzleti* hírszerzés, bűnözés, terrorista csoportok, valamint aktivista egyének vagy csoportok.

A fenti veszélyek következtében a közigazgatás és a társadalom működését lehetővé tevő *informatikai infrastruktúrák*, az informatikai rendszerek vezérlésére támaszkodó nemzeti *létfontosságú infrastruktúra*, illetve a nemzeti *adatvagyon* védelme, a kiberbiztonság fenntartása kiemelt feladattá vált. Ennek következtében alapvető kormányzati igénnyé és egyben feladattá emelve a kiberbiztonság szavatolását. Az állam kiberbiztonsága az információs társadalmak biztonságának szerves része lett: kiberbiztonság nélkül nem képzelhető el sem a nemzeti adatvagyon, sem az államműködés szempontból létfontosságú infrastruktúrák biztonságos működtetése.

E korszak meghatározó jelentősége, hogy a nemzeti adatvagyon és a létfontosságú infrastruktúrák működésének kibertérbeli fenyegetettsége és sebezhetősége, olyan szintre emel-

kedett, hogy egy infokommunikációs katasztrófa valószínűsíthetően ugyanakkora vagy akár nagyobb károkat képes okozni a nemzeti szuverenitás fenntartásának védelme tekintetében, illetve a nemzetgazdaság működése szempontjából, mint a hagyományos biztonságpolitikai potenciális fenyegetettségek, vagy egyes természeti katasztrófák.

A kibertérben megjelenő *veszélyek* és a lehetséges *óvintézkedések* számbavételével határozható meg a kiberbiztonság jelentése. A kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és biztonsági tudatosság növelő módszerek és eszközrendszer, valamint *műszaki, informatikai eszközök* folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok mérséklésével, a kockázatok elfogadható szintjét megteremtve, a kiberteret viszonylagosan megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetése végett.

A *kibertérben* potenciálisan létező *veszélyek* nem pusztán virtuális fenyegetések. E fenyegetések hatást váltanak ki a fizikai világban is, mivel a kibertérhez kapcsolódó kommunikációs, irányító és ellenőrző rendszereiken keresztül a *létfontosságú* rendszerek és létesítmények folyamatos és biztonságos működése nagymértékben függ a kibertér biztonsági helyzetétől. **Biztonságpolitikai** szempontból egyértelműen érzékelhető, hogy a biztonság- és védelempolitika *szárazföldi*, *légi*, *tengeri* és *űr* dimenziója mellett a *kibertér*, mint az ötödik biztonságpolitikai dimenzió jelenik meg.

A kibertérben zajló tevékenység részéről kiváltott hatások révén, a kibertér elérkezett arra a gazdasági és politikai befolyásolási képességi fokra, amely már jelentős hatást gyakorol a fizikai valóságra is. Ennek következtében a *kibertér biztonságának* kérdése arra a nemzeti biztonságpolitikai szintre emelkedett, hogy a kibertér a korábbi technikai részletszabályok helyett átfogó és összetett szabályozást igényel. A Magyarországgal szövetséges NATO államokban, valamint az EU tagállamokban is kormányzati koordinációs szervezetek alakultak, együttműködési fórumokat alapítottak a közigazgatás, a gazdasági (üzleti), a tudományos (akadémiai) és civil szférák között. Ezek az államok szakosított intézményeket működtetnek a kibertérrel összefüggő kérdések vonatkozásában. E szervezetek kiberbiztonsági stratégiákat hoznak létre, kiberbiztonsági törvényeket fogadnak el, nemzeti és nemzetközi kiber válságkezelési mechanizmusokat és együttműködéseket alakítanak ki; biztonságtudatosító és képzési programokat indítanak be, valamint üzleti alapon ösztönzési rendszereket alakítanak ki a nemzeti kiberbiztonsági helyzet javítására.

A **Nemzeti Kiberbiztonsági Stratégia** gyökereiben a 2001-ben elfogadott ún. „**Budapest Konvenció**”-ig nyúl vissza, amely egyrészt nemzetközi fontosságú konkrét magyar hozzájárulás a globális kiberbiztonsághoz, másrészt napjainkig az egyetlen *nemzetközi jogi szerződés* e területen, amelyet hivatkozási alapnak lehet használni. Az *Egyezményben* megfogalmazott alapelvek mindmáig érvényesek, és nemzetközi szinten is széles körben elfogadottak.

A stratégia alapelve az átfogó és összehangolt megközelítés:

- melyben kormányzati és nem-kormányzati, katonai, rendvédelmi és civil, nemzeti és nemzetközi, gazdasági és politikai eszközök egyaránt megfelelő hangsúllyal szerepelnek,
- ahol a felelősségek, feladat és hatáskörök pontosan, összehangoltan fogalmazódnak meg,
- amely a kormányzati és a magánszféra önkéntes együttműködésére, önkéntes információ-megosztásra építve a kormányzat és az érintett szférák közös erőfeszítésével kerül megvalósításra.

A stratégia alapvető célja, hogy Magyarországon az informatikai eszközök, rendszerek és szolgáltatások, valamint az elektronikus hírközlési infrastruktúra és szolgáltatások üzembiztosak legyenek, továbbá megfelelő szintű felkészültséggel és védelemmel rendelkezzenek a kiberfenyegetések és kibertámadások ellen.

Az ***elektronikus információbiztonságról szóló törvény*** a kormányzati koordináció céljából a **Nemzeti Kiberbiztonsági Koordinációs Tanács** (a továbbiakban: **Tanács**) létrehozásáról rendelkezik. E *Tanácsot* a Miniszterelnökség irányításával az érintett minisztériumok és hatóságok bevonásával hozzák létre. A Tanács tevékenységén keresztül elősegíti a kiberbiztonság szabályozását, támogatja a források hatékony felhasználását, felügyeli a nemzeti kiberbiztonsági stratégia és az akcióterv teljesülését, folyamatosan követve a kibertér változásait, szükség esetén javaslatot tesz a stratégia és az akcióterv megújítására. A Miniszterelnökség által delegált *kiberbiztonsági koordinátoron* keresztül ellátja az egységes magyar álláspont kialakítását és képviseletét a nemzetközi politikai együttműködésekben.

Háborús helyzetben a háborús vezetési rend egységességének elvéből kiindulva a Magyar Honvédség látja el a kiberműveleti tevékenységek országos koordinálását, ideértve úgy a katonai, mint a polgári célú kommunikációs és információs rendszerek védelmének irányítását.

A megelőzés, felkészülés és ellenőrzés minden esetben elsősorban az érintett szervezet saját felelőssége. Ezek megtámogatására és megerősítésére azonban ún. szakosított intézményeket szükséges működtetni. Ilyen speciális szakértelemmel és hatáskörrel rendelkező szakegység a rendőrség, valamint a *Nemzeti Adó- és Vámhivatal* szervezeti keretein belül is működik a *számítógépes bűnözés* elleni harcra szakosodott egységek formájában, valamint az Országos Katasztrófavédelmi Főigazgatóságon a kritikus infrastruktúrák informatikai védelméért felelős szervezeti egység keretében. Ilyen szervezet a Nemzeti Biztonsági Felügyelet is, amely sérülékenység vizsgálatot végez. Magyarország nemzetbiztonsági szolgálatai a kibertérben fellépő fenyegetések elhárítására és információszerzésre szakosodott szervezeti egységeket alakítottak ki. A Magyar Honvédség ellátja a katonai célú kommunikációs és információs rendszerek működtetését és védelmét, fokozatosan alakítja ki kibervédelmi képességeit, felhasználva az önkéntes tartalékos rendszerbe jelentkező szakértőket is. Mindezen szakosított intézmények munkáját a Nemzeti Média és Hírközlési Hatóság, mint szakhatóság, kormányzati felkérésre segítheti. Az említett szervezeteken kívül további közigazgatási szervezetek és állami intézmények látnak el a hatásköri jogszabályokban lefektetett kiberbiztonsági feladatokat.

A kiberbiztonsági események operatív kezeléséhez kapcsolódó alapfeladatot lát el az európai kormányzati incidenskezelő csoport (**European Governmental CERT Group**) által minősített kormányzati eseménykezelő központ, valamint ágazati esemény- illetve incidenskezelő központok (CERT-teket). Kiemelendő, hogy a szakosított intézmények kiberbiztonsági tevékenységük során együttműködnek a személyes adatvédelem és a titokvédelem kapcsán hatósági feladatokat ellátó hatóságokkal valamint a *Kormányzati Kiberbiztonsági Koordinációs Tanáccsal*.

A magyar kibertér biztonságának szabályozása több lépésben történik meg. Elsőként a *létfontosságú rendszerek és létesítmények* azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvénnyel Magyarország gondoskodott a kritikus infrastruktúrák védelméről, érintve azok hálózatbiztonsági követelményeit. Második lépésben a *kormányzati elektronikus információbiztonság területe* kerül szabályozásra, amely felhatalmazást ad a kapcsolódó végrehajtási szabályok kormányrendeleti és/vagy miniszteri rendeleti szintű további szabályozására. Ezen jogszabályokat egészítik ki azok az operatív együttműködési megállapodások, melyek egyrészről a kormányzati szervek közötti munkafolyamatokat rendezik,

másrészt a magyar kibertér nem kormányzati tényezői és a kormányzati szervek közötti kapcsolatok jogalapját teremtik meg.

A nemzetközi együttműködés területén igen sikeres és elismert Magyarország eddigi részvétele a különböző nemzetközi együttműködési struktúrákban, többek között:

- az Európai Unió tagországai által önkéntes alapon szerveződött Európai Kiber Válság Együttműködési Keret (European Cyber Crisis Cooperation Framework) munkacsoportjában,
- az Európai Hálózati és Információbiztonsági Ügynökség, az ENISA által kialakított képességfejlesztő együttműködésekben,
- az International Watch and Warn Network tagállamok „kibervihar" (Cyberstorm) típusú nemzetközi együttműködései keretében lezajlott nemzetközi gyakorlatokon,
- a Meridian konferenciasorozathoz hasonló kormányzati együttműködésekben.

A tudatosság növelése és a megfelelő szakemberek biztosítása érdekében kiemelt figyelmet kell fordítani arra, hogy az oktatás minden területén megjelenjen a kiberbiztonsági képzés. Speciális képzési formát igényel a kormányzati tisztviselők alap- illetve továbbképzése, annak érdekében, hogy az informatika szakterületen dolgozó kormányzati tisztviselők megfelelő tudás birtokában képesek legyenek az e-közigazgatást egyre szélesebb körben alkalmazó magyar közigazgatás elektronikus információs rendszereinek biztonságos működtetésre. A *Gyermekbarát Internet Európai Stratégiájának* célkitűzéseivel összhangban kiemelten fontos területként szükséges kezelni a gyermekvédelmet.

2.2 Európai Unió- kibertér, adatvédelem és információbiztonság

AZ EU tagállamok kormányzatainak a következő szempontokat kell figyelembe venni a szabályozás kialakítása során.

1. **Területi elv**. szabályozásnak egyértelművé kell tennie, hogy ha nem-európai (EU tagállami) cégek informatikai, számítási felhő szolgáltatásokat ajánlanak EU tagállami fogyasztóknak, akkor szigorúan alkalmazniuk kell az EU adatvédelmi és adatbiztonsági szabályozásait, az adatok begyűjtésének pillanatától, az adatok teljes megsemmisítéséig.
2. **Nemzetköz adatátadás**. A szabályozásnak ki kell alakítani azt a feltételrendszert, amelynek fennállása esetén EU tagállami kiszolgáló gépről (szerver) USA-beli kiszolgá-

ló gépre lehet adatot továbbítani. Ez az adatátadási, információszállítási mód, amely az EU-n kívülre viszi az adatokat és az USA NSA hatáskörébe juttatja.

3. **Betarthatóság, kikényszeríthetőség**. Az új szabályozásnak szigorú büntetési tételeket kell tartalmaznia, (pl. az érintett cég árbevételének 2%-a lehet a büntetési tétel) az EU szabályozás megsértése esetére. Jelenleg ha a cégek és az EU szabályozás között összeütközésre kerül sor, az EU-n kívüli cégeknek nincs okuk az aggodalomra, és a szabálysértés elkerülésének megfontolására. Egy ilyen szabályozás esetén azonban kétszer is meggondolnák, hogy a törvénysértést válasszák.

4. **Adatfeldolgozók**. Az új szabályozásnak a számítási felhőszolgáltatók esetében világos és egyértelmű szabályokat kell megfogalmaznia a kötelezettségek és felelősségek tekintetében; felhőszolgáltatók valójában adatfeldolgozóknak tekinthetők amagyar jogi terminológiában. A PRISM rendszer rámutatott, arra, hogy lehetőség van széles sugárutat nyitni azok számára, akik hozzá akarnak férni az adatokhoz.

A jelenlegi EU szintű szabályozás nagyon bürokratikus. Ezért a szabályokat egységes, egyszerűsített keretbe kellene elrendezni, amelyet az EU tagállamok mindegyikében egységesen kellene alkalmazni. Jelenleg a 28 EU tagállam esetében egy informatikai és/vagy számítási felhő szolgáltatónak 28 különböző, nemzeti törvénnyel kell szembenéznie. Egyes törvények és szabályozási környezetek rendkívül összetettek. Németországban az EU adatvédelmi törvényt értelmező rendelkezések leírása 60 oldalra rúg. Ha vesszük ezt a 60 oldalt mint referencia pontot, akkor a 28 tagállammal megszorozva egy áttekinthetetlenül nagy és bonyolult joganyagot kapunk. Ez érzékelteti e kérdés szabályozási bonyolultságát.

Az EU adatvédelmi szabályainak kialakítását már több mint két éve vitatják az EU-n belül. Talán most kialakítható valamilyen konszenzus és egyezség annak érdekében, hogy megvédjék az Eu polgárokat a nem kívánt megfigyelésektől.

2.3 Számítási felhő

A ***PRISM***-botrány miatt ugyanakkor még inkább felértékelődött az adatbiztonság, illetve az adatvédelem kérdése, emiatt felgyorsulhat az *új Európai Uniós adatvédelm*i szabályozás elfogadása. Az EU pedig 2013-ban meghirdetett Európai Cloud Partnerség keretében igyekszik

kiépíteni az "európai számítási felhőt", és a tervezett jogi keretrendszerrel erősítené a számítási felhő szolgáltatások iránti bizalmat a felhasználók körében.

> *Az amerikai Nemzetbiztonsági Hivatal (NSA) gyakorlatilag korlátlanul hozzáfér a nagy amerikai online szolgáltatók (Google, Yahoo, Facebook, Microsoft, AOL) szerverein tárolt emailekhez, szöveges, hangalapú és videós beszélgetésekhez, tárolt fotókhoz és videókhoz, elküldött fájlokhoz, videókonferenciákhoz, közösségi tevékenységekhez, feltöltött fájlokhoz. A PRISM program keretében az NSA-val együttműködő vállalatok (USA) önkéntes módon csatlakoztak a megfigyelési rendszerhez és adtak hozzáférést a náluk tárolt adatokhoz az ügynökségnek - ezt a megnevezett cégek egyébként mind tagadták.*

Az USA-ban a törvényi alapot a Foreign Intelligence Surveillance Act (FISA) 702 cikkelye adja meg. Az USA kormány tisztviselők szerint ez egy kormányzati belső számítógépes rendszer, amely a kormányzat számára gyűjt hírszerzési információkat elektronikus szolgáltatásokból, bírósági felügyelet alatt.

A Boston Consulting Group szerint az EU állampolgárokról összegyűjtött adatok értéke 315 milliárd €-t érte le 2011-ben. A tendencia azt mutatja, hogy 2020-ra, ez az érték 1 billió €-ra rúghat. Ez tény az adatvezérelt és adatközpontú gazdaság és gazdálkodás jelentős szerepét mutatja, és azt, hogy a bizalom megingása, súlyos veszélyekkel járna az egész gazdaság tekintetében.

Ebben a kontextusban a számítási felhő és a számítási felhőben elhelyezett adatok kényes kérdéssé váltak. Bár a bizalom tekinthető egy fajta valutának és pénzügyi csereérték kapcsolható hozzá, az USA nemzetbiztonsági felderítésével összefüggő információk nyilvánosságra kerülése, és a személyes és üzleti adatok védelmével összefüggő aggodalmak jelentős felerősödése odavezetett, hogy a Számítási Felhő Biztonságáért Dolgozó Szövetség (Cloud Security Alliance) felmérése szerint a választ adók 56% jelentős ellenérzéseket fejezett ki abban a tekintetben, hogy USA-bázisú szolgáltatót használjon fel számítási felhő szolgáltatások igénybevétele esetén. Ezek a tények rámutatnak arra, hogy EU tagállamok kormányzataiban szükség van az attitűd megváltoztatására. A felmérés eredményéből az volt becsülhető, hogy az amerikai számítási felhőszolgáltatók az elkövetkező három évben 22-36 milliárd USA dol-

lár bevételtől eshetnek el. (The Information Technology and Innovation Foundation becslése).

Ez azt is jelentheti, hogy az EU szolgáltatók jelentős versenyelőnyre tehetnek szert, a sokkal szigorúbb adatvédelmi és adatbiztonsági előírások és szabályozások környezetében, amelyeket be kell tartaniuk.

3 INFORMÁCIÓ BIZTONSÁGI„PROGRAM”

Az információbiztonsági vezetőnek akár az információbiztonsági program kialakításához, akár tényleges megvalósítás és vezetéséhez sok olyan szervezési és vezetési, valamint igazgatási, szervezet folyamat fogalmat kell megértenie és aktív tudásként használnia, amelyek közül a lényegessebbeket, nem teljes, és nem kimerítő, listaszerű felsorolás fomájában az alábbiakban láthatók:

1. Szoftverfejlesztési életciklus modellek (SDLC-k);
2. Követelményelemzés, kialakítás;
3. Követelmény, rendszer specifikáció kidolgozás;
4. Óvintézkedések, ellenőrzési mechanizmusok, kontroll célkítűzések;
5. Az óvintézkedések, ellenőrzési mechanizmusok, kontrollok megtervezése és kifejlesztése;
6. Az óvintézkedések, ellenőrzési mechanizmusok, kontrollok bevezetése és tényleges megvalósítása;
7. Az óvintézkedések, ellenőrzési mechanizmusok, kontrollok nyomon követése, felügyelet, monitorozása és aklamas indikátorok, mutató- és mérőszámok, metrikák kialakítása;
8. Architektúra megfogalmazása és kialakítása;
9. Dokumentáció: a szüséges és előállítandó dokumentumok;
10. Minőségbiztosítás;
11. Projektirányítás;
12. Beruházási, befektetési, üzleti tervek kialakítása: beruházás megtérülés, költség, haszon elemzés;
13. Ellenintézkedések
14. Technológia
15. Alkalmazottak, szerepkörök/munkakörök/felelősség/hatás és feladatkörök, képesség, szakmai képzettség
16. Folyamatmenedzsment, folyamatszervezés, folyamatok újratervezése,atutomatizált munkafolyamatok, munkafolyamatok szervezése (BPM/BPR, Business Process Management, Business Process Re-engineering, Workflow).
17. Költségvetés készítés, költségbecslés és pénzügyek;

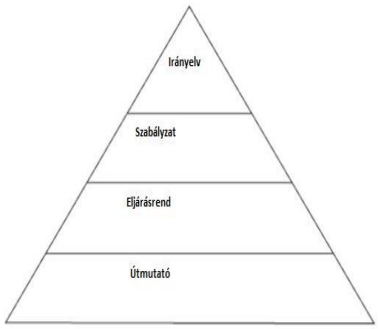
18. Rendszer telepítése, üzembehelyezési és integráció stratégiák;
19. Képzési igények és oktatás felmérése, értékelése és lehetséges megoldási módok;
20. Tájékoztatás (kommunikáció);
21. Problema kezelés, megoldás;
22. Kockázat kezelés;
23. A szabályszerűség, megfelelőség nyomon követése, felügyelete, ellenőrzése és betartatása;
24. Személyzeti ügyek.

Az információbiztonsági vezetőnek szervezési szinten jártasnak kell lennie az informatikai technológiákban; a létfontosságú technológiákból vett példahalmazt láthatunk alább:

1. Tűzfalak;
2. Vírusvédelmi rendszerek;
3. A hálózati aktív eszközökben fellehető informatikai biztonsági sajátosságok (pl. útvonalirányítók (router), switch stb.);
4. Behatolás észlelő rendszerek (IDS, Intrusion Detection Systems, gazdagép alapú, hálózati; host-based, network).
5. Behatolást megelőző rendszerek (Intrusion Prevention Systems);
6. Kriptográfiai eljárások (pl. PKI, nyilvános/publikus kulcsú infrastruktúra, Advanced Encrytion Standard (AES);
7. Elektronikus, digitális aláírás;
8. Intelligens kártyák (Smart cards);
9. Hitelesítési és engedélyezési eljárások (Authorization, Authentication)[Egy alkalomra érvényes jelszó (OTP), kihívás-válasz (challenge-response), PKI tanúsítványok, több faktoros azonosítás, biometrika];
10. Mobil eszközök;
11. Vezeték néküli hálózatok biztonsági kérdései;
12. Alkalmazás fejlesztések biztonsági módszerei;
13. Távoli hálózat elérési módszerek (VPN, Virtual Private Network);
14. Web biztonsági technikák és megoldások;
15. Naplókészítés, napló elemzése és elemző eszközök (pl. biztonsági információk és események kezelő eszköze, Security Information and Even Management [SIEM]).

16. Sebezhetőség kereső és behatolási lehetőségeket tesztelő eszközök (Vulnearbility scanning, penetration testing).
17. Adatszivárgást megelőző módszerek (eltávolitható adathordozó eszközök biztonsági feltételei, tartalomszűrés, stb.), és szomszédos technológiák;
18. Adatintegritásra vonatkozó óvintézkedések (adatok épsége, sértetlensége); mentés, adat pillanatfelvétel (snapshot), adattükrözés, RAID? SAN, valós-idejű tükrözés stb.
19. Azonosítási hozzáférési engedélyek, jogosultságokat kezelő rendszerek.

Sok és különböző forrásra van szükség egy *informatikai/információ biztonsági program* kialakításához. Egy információbiztonsági vezetőnek értenie kell, hogy mik ezek a forrásanyagok és azokat hogyan lehet felhasználni az információ biztonsági célok elérése érdekében.



1. ábra A dokumentáció szerkezete

Az információbiztonsági vezetőnek az információ- és informatikai biztonsági architektúrákon és technológiákon kívül a szélesebb értelemben vett információtechnológiai eszközöket és technológiákat is ismernie kell, amelyek közé az alábbi tartoznak ismét példálózó jellegű felsorolással:

1. Heliy hálózatok (LAN, Local Area Network);
2. Nagy távolságú hálózatok (WAN? Wide Area Network);
3. Mentési és archiválási eljárások mint például a RAID (redundant array) illetve SAN (storage area network).
4. Internet és hálózati protokollok (TCP/IP, UDP, stb.);
5. Operációs rendszerek;
6. Útvonalirányítás az info-kommunikációs hálózatokon és protokollok;
7. Adatbázis kezelő rendszerek;

8. Kiszolgálók (Servers);
9. Vállalati szervezeti architektúra (két, három szintű ügyfél kiszolgáló [kliens-szerver], üzenettovábbító és üzenetkapcsolt rendszerek, stb.).
10. Virtualizáció;
11. Számítási felhő;
12. Web technológiák és architektúrák.

Architektúra magas szintű, az architektúrális építő elemek közti kapcsolatok fogalmi szintű leírása, a technológiai architektúra résteg legfontosabb építőelemei:

Hálózati topológia;

Alkalmazási rendszerek;

Köztes rendszerek /szoftverek;

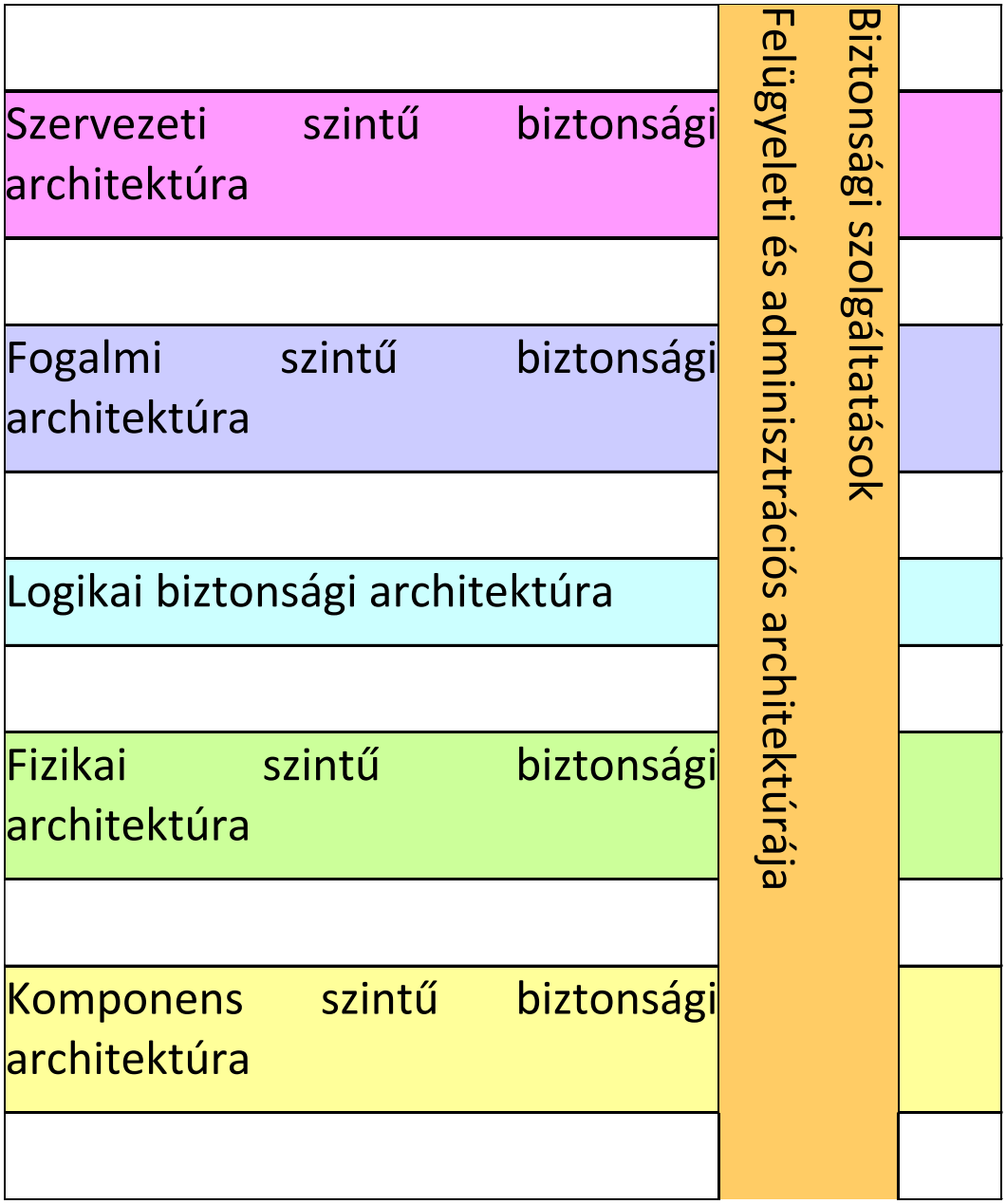
Csúcstechnológiai kütyük;

Operációs rendszerek;

Egyéb berendezések.

Az architektúra a technológiai eszközök sajátosságainak és funkcionális szolgáltatásainak magas szintű leírását tartalmazza, amelynek segítségével a kívánt funkcionális szolgáltatások megtervezhetők és összeépíthetők.

Megvalósítási lehetőségek:



2. ábra SABSA alap architektúra szerkezete

Szervezeti szintű réteg	Szervezeti motivációk, hajtóerők kialakítása; szervezeti szintű kockázatok elemzése, értékelése; szolgáltatáskezelés, kapcsolatkezelés, teljesítménykezelés, beszállítói, ellátási hálózat kezelése.
Fogalmi szintű réteg	A szervezet **sajátosságai profiljának kialakítása**, működési kockázati kezelés célkitűzéseinek kidolgozása a kockázat elemzés segítségével, szolgáltatásnyújtásra tervkészítés, szolgáltatási szerep /feladat /munka /felelősség /hatáskörök, szervezeti kultúra értéktételezéseinek meghatározása, szolgáltatás portfólió kezelés, a szolgáltatási katalógus megtervezése, napra készen tartása, a szolgáltatások teljesítmény kritériumainak és célkitűzéseinek kezelése (szolgáltatási szintek meghatározása).
Logikai réteg	Informatikai vagyon/ tárgyi eszközkezelés, irányelvek/ házirend kezelése, szolgáltatásnyújtás kezelésem ügyfélszolgálat, szolgáltatás katalógus kezelése, és a szolgáltatás értékelés kezelése.
Fizikai szintű réteg	Informatikai vagyon/ tárgyi eszköz biztonsága és védelme, működési kockázatokra vonatkozó adatok gyűjtése, üzemeltetés, felhasználó támogatás, szolgáltatási erőforrások védelme, szolgáltatás teljesítmény adatok gyűjtése.
Komponens szintű réteg	Eszközök védelme, üzemeltetési / működési kockázatokat kezelő eszközök, eszközök telepítése, alkalmazottak delegálása, biztonsági eszközök, szolgáltatás monitorozó, felügyeleti eszközök.

3. ábra A biztonsági szolgáltatások kezelésének architektúrája

Szakterületek együttműködése

A szervezeti architektúra

Funkcionális/üzleti architektúra

Információs architektúra

Alkalmazási architektúra

Szervezeti biztonsági architektúra

Műszaki architektúra

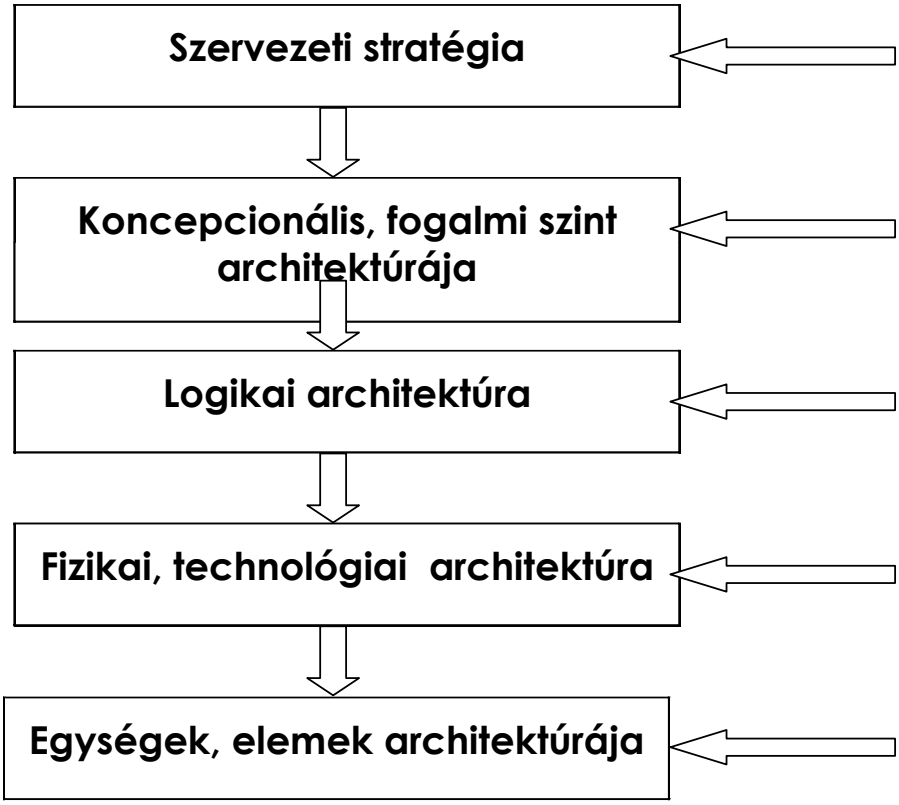
Termék architektúra

J. A. Zachman S. H. Spewak keretrendszer	Biztonsági architektúra		
Tervkészítő (szervezeti/üzleti/stratégia) célkitűzések/kiterjedés	Üzleti vetület (összefüggések)	Miért?	Szervezeti biztonsági stratégia
Tulajdonos, vezető Szervezeti modell	Szervezeti vetület (irányelvek)	Mit?	Szervezeti politika, biztonsági, Irányelevek architektúrája
Fejlesztő Információs rendszer modell	Tervezői vetület	Hogyan?	Logikai architektúra
Kivitelező Technológiai modell	Kivitelezői vetület	Hogyan, hol?	Fizikai, technológiai architektúra
Végrehajtó (alvállalkozó) Részletes specifikáció	Integrációs vetület	Mivel?	Egységek, elemek architektúrája
Működő vállalat/intézmény	Üzemeltetési vetület	Ki, mikor?	Működtetési architektúra

4. ábra Miért? Mit? Hogyan? Hol? Ki? Mikor?

.	Eszközök (Mit?)	Folyamatok (Hogyan?)	Helyszínek (Hol?)	Emberek (Ki?)	Idő (Mikor?)	Motiváció (Miért?)
Szervezeti vetület (Összefüggések rétege)	**Mi a rendszer típusa, mi a terméke? A cég védendő értékei: jó hírnév védelme, a védendő információk**	**Hogyan működik? A védendő üzleti folyamatok (tranzakciók, kommunikáció)**	**Hol működik? Zárt rendszer, több telephely, külső partnerek, nyílt, országos /nemzetközi kapcsolatok**	**Ki használja? Szervezeti és menedzselési kérdések, ellátási lánc, stratégia partnerek, outsourcing**	**Mikor használja? Határidők, ciklusok, azonnali igények, terhelés megoszlás, csúcsok**	**Miért használja? Üzleti célok, sikertényezők, működési kockázatok**
Szervezeti architektúra vetület (Koncepciók rétege)	**Mit kell megvédeni? Üzleti titok, szervezeti egységek, kapcsolataik**	**Hogyan működjön a védelem? Felső szintű biztonsági straté-giák: PKI, alkalmazás védelem**	**Hol vannak a vé-dendő területek? A védelem helyfüggősége, biztonsági domainek**	**Ki menedzsel? Menedzselés szervezeti modell-je: biztonsági hatóságok, PCA, CA, RA**	**Mikor kell a védelem? Időpont, tartam? Jelszó, tanúsítvány élet-ciklus, CLR idő**	**Miért fontos? Szervezeti kocká-zat elemzés, sebezhetőség és költség hatékonys**
Tervezői vetület (System engineering, Logikai réteg)	**Védendő adatentitások és kapcsolatuk, PKI tanúsítvány, CA**	**Biztonsági szolgáltatások: hitelesség, teljesség, letagadhatatlans**	**Védelmi terület definiálása, biztonsági domainek logikai, fizikai, stb.**	**A jogosultsági profilok: felhasználó, rendszergazda, auditor**	**A biztonsági folyamat ciklusa jogosultság, tanú-sítvány kiadáskor**	**Biztonsági politikák követelményei, CPS, helyi domain pol.**
Kivitelezői vetület (Fizikai réteg)	**Védendő adatstruktúrák: üzenetek, táblák, elektr. aláírások**	**A biztonsági me-chanizmus: titko-sítás, vírus véde-lem, AC szerverek**	**A biztonságtech-nológiai infra-struktúra elemeinek helye**	**Biztonsági felhasználói interfé-szek képernyő formája**	**Az ellenőrzési rendszer működtetéséne k időrendje**	**Biztonsági szabályok, feltételek és tevékenységek**
Inegrációs vetület (Elemek rétege)	**Adatmezők és címek részletes specifikációja**	**Termék és eszköz: hardver, szoftver és a vonatkozó szabványok**	**Számítógépes fo-lyamatok, cso-mópontok címei és protokollok**	**Felhasználói azonosítók, kivé-telek és ACL-ek**	**Biztonsági tevékenységek időtartama és sorrendje**	**Biztonsági tevékenységek és intézkedések**
Üzemeltetési vetület, réteg	**Üzemeltetési biztonság: bizalmasság, teljesség, authentikusság**	**Felhasználók és rendszerek biztonsági adminisztrációj a, mentések,**	**Hálózatok és plat-formok biztonsá-ga a szabványok alkalmazásával**	**Felhasználók, operátorok és adminisztrátoro k támogatása**	**Biztonsági tevékenységek időbeosztás sze-rinti végzése**	**Az üzemeltetés folyamatosságá -nak és biztonságának fenntartása**

5. ábra Az IT tervezés Zachman féle keretrendszere



6. ábra Biztonsági architektúra modellje

Az ellenőrzési mechanizmusok mint a megvalósítás stratégiájának forrásai

Az ellenőrzési mechanizmusok:

irányelvek, eljárásrendek, napi gyakorlat/rutin, műszaki megoldások, technológiák, és szervezeti felépítés, amelyet arra terveztek, hogy ésszerű garanciát nyújtson a következő tekintetében:

A szervezeti/üzleti/igazgatási célkitűzéseket el fogják érni

A nem kívánt eseményeket meg fogják akadályozni, vagy észlelni fogják, és a következményeket pedig korrigálják

Az ellenőrzési mechanizmusokat és az óvintézkedéseket amennyira az csak lehetséges automatizálni fogják

SABSA mátrix - Biztonsági szervezeti architektúra (ld. 2. ábra)

Ellenintézkedések, óvintézkedések:

Az ellenintézkedések, óvintézkedések, olyan ellenőrzési mechanizmusok, amelyeket olyan fenyegetésekkel szemben hoznak létre, amelyek előre tudhatók.

Az ellenintézkedések és óvintézkedések a következők lehetnek:

Megelőző

Észlelő

Helyre állító /korrigáló

Technológiák

A szervezet elavult technológiájú architektúrája behatárolja azoknak a technológiáknak a körét, amelyeket fel lehet használni a biztonsággal kapcsolatos kockázatok mérséklésére.

Az elmúlt évtizedekben felhalmozódott tapasztalatok az alternatív technológiák értékelésében, a megelőző, észlelő és helyreállító ellenőrzési mechanizmusok tekintetében, amelyek célja az információ biztonsági célok megvalósítása, ma már széles körben rendelkezésre állnak. Általában használt technológiák:

Hozzáférési jogosultsági lista:

Rendszer konfiguráció állományok, amelyek az azonosított és hitelesített rendszer használatot lehetővé teszik, azonban megakadályozzák a jogosulatlan rendszer felhasználást.

Lefojtó útvonal irányító:

Hálózati eszközök, amelyek két hálózat közötti átjáróként szolgálnak, és csak olyan adatforgalmat engednek át, amely az előre definiált szabályrendszernek megfelel.

Tartalom szűrés:

Az állományok tartalmának vizsgálata annak érdekében, hogy megakadályozzák azt, hogy az állomány az ellenőrzési ponton túljutva károkat okozhasson. A szabályrendszer szerint vagy továbbengedik, vagy megakadályozzák a belépését a rendszerbe.

Adatbázis-kezelő rendszerek:

Az adatok tárolásának és visszakeresésének hatékony technológiája, amely előredefiniált indexelési eljárást alkalmaz, amely meghatározza, hogy melyek az egyes adatrekordok

Sifrírozás, rejtjelezés, kriptográfiai, algoritmikus információ védelem (*nyilvános kulcs*, *szimmetrikus* vagy titkos kulcsú *sifrírozás*):

> Olyan algoritmus, amely az információ elrejtésére szolgál olyan módon, hogy csak azok ismerhessék meg, akik erre illetékesek, és az eredeti formát vissza tudják állítani.
>
> Az információ *titkosságának*, *bizalmasságának* megőrzésére szolgál, továbbá az adatok *épségének*, *sértetlenségének* (integritás) és *letagadthatatlanságának* ellenőrzésére. (CIA, Confidentiality, Integrity, Accesibbility).

Zagyválás („Hash-elés”)

> Olyan algoritmus, amely tetszőleges adatbemenetre egy szabványosított hosszúságú kimenetet hoz létre, amely elfedi az eredeti üzenetet, és ezt az algoritmust nem lehet felhasználni az eredeti üzenet rekonstruálására, de ugyanarra az üzenetre ugyanazt az eredményt adja

Open Systems Interconnection (OSI) modell

> A hálózati kommunikáció egyik szabványa, amely leír egy keretrendszert a hét rétegen belül megvalósítandó protokollok számára

Applikációs (alkalmazási) réteg: Az applikációk (fájlátvitel, e-mail stb.) működéséhez nélkülözhetetlen szolgáltatásokat biztosítja.

Megjelenítési (prezentációs) réteg: Feladata a különböző csomópontokon használt különböző adatstruktúrákból eredő információ-értelmezési problémák feloldása.

Viszony réteg: Ez a réteg építi ki, kezeli és fejezi be az applikációk közötti dialógusokat (session, dialógus kontroll).

Szállítási réteg: Megbízható hálózati összeköttetést létesít két csomópont között. Feladatkörébe tartozik pl. a virtuális áramkörök kezelése, átviteli hibák felismerése/javítása és az áramlásszabályozás.

Hálózati réteg: Összeköttetést és útvonalválasztást biztosít két hálózati csomópont között. Ehhez a réteghez tartozik a hálózati címzés és az útvonalválasztás (routing).

Adatkapcsolati réteg: Megbízható adatátvitelt biztosít egy fizikai összeköttetésen keresztül. E réteg probléma köréhez tartozik a fizikai címzés (hálózati topológia fizikai címzési rend-

szer), közeghozzáférés, fizikai átvitel hibajelzése és a keretek sorrendhelyes kézbesítése. Az IEEE két alrétegre (MAC, LLC) bontotta az adatkapcsolati réteget.

Fizikai réteg: Elektromos és mechanikai jellemzők procedurális és funkcionális specifikációja két (közvetlen fizikai összeköttetésű) eszköz közötti jeltovábbítás céljából.

Operációs rendszer

Egy olyan progam, amely közvetlenül kapcsolódik a hardverhez, és lehetővé teszi a szoftverek futtatását. Az operációs rendszer „edzése, keményítése" („hardening") kulcsfontosságú biztonsági kérdés: fontosabb elemek FTP, TELNET, távoli rendszer elérések ellenőrzése (Remote Access, Terminal), Kerberos (kerenlbeli és kivüli elemek), stb.

Néhány biztonsági szolgáltatás: részletes és megbízható naplózási mechanizmus, állomány (file) rendszer.

Nyilvános kulcsú sifrírozás (PKI, Public key kriptográfia):

A Nyilvános kulcsú sifrírozás egy olyan kriptográfiai algoritmus, amely két kulcsot használ, a nyilvános és magánkulcsot. Az egyiket használja a sifrírozásra, a másikat a visszafejtésre.

Szimmetrikus kulcsú sifrírozás

Olyan kriptográfiai algoritmus, amelyben a kulcsot mind sifrírozásra mind visszafejtésre használjuk.

Útvonal szűrés

A hálózati eszközök olyan programozása, amely egy előre meghatározott hálózati cím halmazból engedi meg vagy hálózati forgalom befogadását vagy oda a továbbítását. Ha egy adott eszköz számára nem létezik ilyen előre definiált útvonal, akkor semmilyen adat nem kerülhet továbbításra abba az irányban.

TCP/IP és IPSec sifrírozás

Számítógép hálózati protokollok halmaza, amelyek az OSI modellre alapulnak. A továbbított adatokat szétbontják fejlécre („*header*") és az adatokra.A fejléc alapján tudják a hálózati eszközök az egyes csomagok esetében az útvonal irányítást végrehajtani a forrás és a célállomás között miközben az adatokat az alkalmazási réteg mint adatfolyamot folyamatosan olvassa be.

Munkatársak, szerepkörök, jogosultságok, felelősség-, feladat-, és hatáskörök, képzettség és képességek témaköre:

Szerepkörök („Role”)

E fogalom lehetővé teszi azt, hogy a hozzáférési jogosultságokat annak alapján lehessen megadni, hogy egy munkatárs vajon melyik funkció végrehajtására jogosult, és nem az egyes munkatársak személyéhez kell kötni

Jogosultságok, felelősség-, feladat-, és hatáskörök („Responsibility”)

A felelősség valamilyen funkció vagy eljárás leírását jelenti, amelynek végrehajtásáért valaki felelősségre vonható.

E felelősség-, feladat-, és hatásköröket ahhoz a szerepkörhöz kell helyezni, ahol a szükséges képzettség, képesség, szakmai gyakorlat fellelhető, a munkatársak fluktuációja ellenére

Képzettség, képesség, szakmai gyakorlat

Elvégzett tanfolyamok, kiképzés, szakértelem és szakmai tapasztalatok, amellyel az adott munkakörben dolgozó alkalmazott rendelkezik

Biztonsági tudatosság

Biztonsági ellenőrzés és kiképzés szükséges ahhoz, hogy a munkafeladatok elvégezéséhez felhatalmazást kapjanak a munka elvégzésére (Ha a képzés elvégzése nem igazolt, nem végezheti el az adott munkát, feladatot, az adott munkakörben).

Biztonsági munkakörökben foglalkoztatandók kiképzésére testre szabott tanfolyamok kialakítása.

A biztonsági tudatosság emelése érdekében a végfelhasználók számára képzés.

3.1 Szervezeti biztonsági architektúra

1. táblázat Architektúra nézetek rétegei (Layered Architecture Views) SABSA © (Sherwood Applied Business Security Architecture)

The Business View	Contextual Security Architecture
The Architect’s View	Conceptual Security Architecture

The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Service Manager's View	Security Service Management Architecture

2. Táblázat SABSA MATRIX (magyar)

	Vagyon/Eszköz(MI)	**Motiváció (Miért)**	**Folyamat(Hogyan)**	**Humán (Ki)**	**Jelyszín(Hol)**	**Idő(Mikor)**
Szervezeti szintű architektúra	*Szervezeti/igazgatási döntések*	*Üzleti kockázatok*	*Szervezeti (vállalati, üzleti)* ***folyamatok***	*Szervezet igazgatása*	*Szervezeti (vállalati, üzleti) földrajzi elhelyezkedése*	*A szervezeti (vállalati, üzleti) tevékenységek időtől való függése*
	Az szervezeti (vállalati, üzleti) vagyon, eszközök, beleértve a célokat és célkítűzéseket	Lehetőségek és fenyegetések leltára	A szervezeti (vállalati, üzleti) müködtetésére szolgáló folyamatok leltára	Szervezeti (vállalati, üzleti) felépítés, és a „kiterjesztett szervezet”.	Az építmények, épületek, telephelyek, tartományok, igazságszolgáltatás, joghatóság kiterjedése, stb.	A szervezeti (vállalati, üzleti) célkitűzések időfüggése
Fogalmi szintű réteg	Szervezeti/vállalati ismeretel, kovkázati stratégia	Kockázat kezelési célkitűzések	A folyamatok korrektségének szavatolása	Jogosultságok, felelősség-, feladat-, és hatáskörök	Keretrendszer számítógéphálózati tartományok-	Az időmenzió kezelésének keretrend-

					ra	szerei
	Szervezeti/vállalati profil attribútumai	Feltételek megteremtése, ellenőrzési célkitűzések, Irányelvek architektúrája	A folyamatok leképezésének keretrendszere: IKT-ra architektúra stratégia	Felelősök „tulajdonosok/gazdák”, gondnokok, végfelhasználók; Szolgáltatás nyújtók és ügyfelek/fogyasztók	Biztonsági tartomány fogalmai é keretrendszerek	Az egész életciklust átfogó kockázatkezelési keretrendszer
Logikai réteg	Információvagyon	Kockázat kezelési irányelvek	Folyamatok és szolgáltatások leképezése, leírása	Entitások és a kölcsönös bizalom keretrendszere	Számítógéphálózati tartományok térképe	Naptár, ütemtervek, menetrend
	Az Információvagyon leltára	Számítógéphálózati tartományokra vonatkozó irányelvek	Információ áramlás; Funkcionális transzformációk; Szolgáltatás központú architektúra	Entitások sémája; Kölcsönös bizalom modelljei; Privilegizált jogosultságok profilja	A tartomáyok meghatározásai; A tartományok közötti kapcsolatok és kölcsönhatások	Indítási időpontok; Élettartam, határidők

Fizikai szintű réteg	Adatvagyon	Kockázat kezelés gyakorlati eljárásai	Szolgáltatási folyamat mechanizmusa	Ember-gép párbeszéd	IKT infrastruktúra	Folyamat ütemezés
	Adatszótár , adatleltár	Kockázat kezelési szabályok és eljárások	Alkalmazások, Köztes rendszerek Biztonsági mechanizmusok	Végfelhasználói felület az IKT rendszerekhez Jogosultság kezelő rendszerek	Gazda platformok, topológia és számítógép hálózatok	Ütemezés, folyamatok és párbeszédek szekvenciális elrendezése végrehajtási célból
Komponens szintű réteg	IKT komponensek	Kockázat kezelési eszközök és szabványok	Szolgáltatási folyamat támogató eszközök és szabványok	Humán erőforrás kezelé eszközei és szabályai	Számítógéphálózat lokációs eszközök és szabványok	Lépések ütemezése, sorrend kialakítását támogató eszközök
	IKT termékek, beleértve az adatokat, repozitóriumokat, adatszótárakat és	Kockázat elemzési eszközök Kockázat katalógus Kockázatok monito-	Szolgáltatás nyújtás eszközöi és protokolljai	Személy azonosság kezelése, munkaköri leírások, szerepkörök; funkciók; Tevékenységek, Hozzáfé-	Csomópontok, címek és egyéb cím azonosítók	Ütemező; óra, időmérő, interrupt kezelő

	folyamataikat	rozása és jelentés készítő eszközök.		rési jogosultsági listák		
Szolgáltatás kezelés architektúrája	Szolgáltatás nyújtás kezelése	Üzemeltetési/működési kockázatok menedzsment	Információfeldolgozási folyamatok menedzsmentje	Humán erőforrás menedzsment	Környezet menedzsment Az épületek, telephelyek, platformok és számítógéphálózat menedzselése	Idő és teljesítmény kezelés
	Az üzemeltetés folyamatosságának és kiválóságának szavatolása	Kockázat becslés, értékelsé; Kockázat monitorozás és jelentés készítés Kockázatokkal való foglalkozás	A rendszerek támogatás, menedzselése, alkalmazások és szolgáltatások	Felhasználó bejegyzésekről gondoskodás Végfelhasználók támogatása	Az épületek, telephelyek, platformok és számítógéphálózat menedzselése	A naptár és menetrend, ütemrend kezelése

3. Táblázat SABSA SERVICE MANAGEMENT MATRIX (Aligned with ITIL v3)

4. Táblázat SABSASzolgáltatás kezelési matrix (ITIL v3-al összehangolva)

	Vagyon/Eszköz(MI)	**Motiváció (Miért)**	**Folyamat(Hogyan)**	**Humán (Ki)**	**Jelyszín(Hol)**	**Idő(Mikor)**
	Szolgáltatás nyújtás kezelése	Üzemeltetési/működési kockázatok menedzsment	Információfeldolgozási folyamatok menedzsmentje	Humán erőforrás menedzsment	Környezet menedzsment Az épületek, telephelyek, platformok és számítógéphálózat menedzselése	Idő és teljesítmény kezelés
	A fentebbi sor a SABSA mátrix 6. sorának megistmétlése. Az alábbi öt sor ammak a kibontása, hogy a 6. réteg hogyan viszonyul a többi réteghez.					
Szervezeti szintű architektúra	A szervezeti (vállalati, üzleti) motivációk, hajtóerők kialakítása	szervezeti (vállalati, üzleti) kockázatok értékelése	Szolgáltatás menedzsment	Kapcsolatartás	A szolgáltatás nyújtási pont menedzselése	Teljesítmény menedzsment
	szervezeti (vállalati, üzleti) összemérés, összehasonlítás,	A belső és külső tényezők elemzése	Az ügyfél számára értéket jelentő szolgáltatás nyújtáshoz szük-	A szolgáltatás nyújtók és a szolgáltatást	Igénykezelés; szolgáltatás nyújtás, telepítés és	szervezeti (vállalati, üzleti) szempontú

	szervezeti (vállalati, üzleti) motivációk, hajtóerők feltárása		séges szolgáltatási kaapcitások menedzselése	igénybevevők kezelése	felhasználás	teljesítmény célok meghatározása
Fogalmi szintű réteg	„Proxy Asset" kialakítása (Információvagyon helyettesítő)	ORM(Opportunity and Risk Method) Lehetőségek és kockázatok módszere céljainak kialakítása	Szolgáltatás nyújtás tervezése	Szolgáltatáa menedzselés szerepkörei Szerepkörök, feladat, felelősség, hatáskörök, meghatározása, pénzbeli kötelezettségek, kulturális értékek	Szolgáltatás portfolió	Szolgáltatási szintek meghatározása (SLA)
	szervezeti (vállalati, üzleti) attribútumok profiljának létrehozása	Kockázat elemzés szervezeti (vállalati, üzleti) attribútumok profiljának, a helyettestő	SLA tervkészítés, üzletvitel, ügymenet folyamatosság,pénzügyi tervezés és ROI		A szolgáltatási katalógus megtervezés és napra	A szolgáltatás teljesítmény szempont-rendszerének

	(=Információvagyon helyettesítő), kulcs fontosságú teljesítmény indikátorok (KPI), kulcs fontosságú kockázati mérőszámo (Key Risk Indicator, KRI)	információvagyon (Proxy Asset) alapján	(Return on Investment), Áttérés tervezés		készen tartása	éscélértékeinek meghatározása
Logikai réteg	Eszköz, vagyon menedzsment/gazdálkodás	Irányelvek kezelése	Szolgáltatás nyújtás menedzsmentje	Szolgáltatás ügyfelének, fogyasztójának támogatása	Szolgáltatás katalógus menedzsment	Kiértékelés
	Tudásmenedzsment, Termék/szolgáltatás kibocsátás és telepítés kezelés; Teszt és validáció menedzsment	Irányelvek kialakítása Irányelvek megfelelőségének ellenőrzése, auditálása	SLA kezelés, Szállítók menedzselése; Üzlet/ügymenet folyamatosság fenntartása; költségek kezelése/ gazdálkodás;Áttérés meendzsment	Jogosultság kezelés, elhasználói jogosultságok. elhasználói bejegyzések kezelése és létrehozása	Konfiguráció kezelés; kapőacitás tervezés; rendelkezésre állás	Monitorozás, nyomon követés, jelentés készíéts; Teljesítmény kontra KPI és KRI

Fizikai szintű réteg	Eszköz/vagyon biztonság védelme	Működési kockázatok adatainak gyűjtése	Üzmeletés/működtetés	Végfelhasználók támogatása	Szolgáltatás erőforrásainak védelme	Szolgáltatás teljesítmény adatok gyűjtése
	Változáskezelése; Szoftver és adat épség/sértetlenség védelme	Működési kockázatok kezelésének architektúrája.	Job ütemezés; Rendkivüli események és események (incidensek) kezelése; Katasztrófa utáni helyreállítás	Szolgáltatás ügyfél szolgálat; Probléma kezelés; Kérelmek kezelése	Fizikai és környezeti iztonság	Rendsze és szolgáltatás monitorozásának architektúrája
Komponens szintű réteg	Eszközök védelme	ORM eszközök	Eszközök telepítése	Humán erőforrás munkába állítása	Biztonsági eszközök	Szolgáltatás monitorozó eszközök
	Termékek és eszközök biztonságának és épségének/sértetlenségéne	ORM elemzés; Monitorozás és jelentés készítés, és megjelenítő eszközök.	Termékek és eszközök kiválasztása, beszerzése; Projekt menedzsment	Munkaerő felvétel Fegyelmi eljárások	Az üzembehelyezett eszközök és termékek fizikai és logikai biztonsá-	Szolgáltatások elemzése, monitorozása, jelentés készítés és megje-

	k fenntartása			Kiképzés Tudatosság erősítő eszközök	gának fenntartása	lenítő rendszerek.

7. ábra Az IT tervezés Zachman féle keretrendszere

	Eszközök (Mit?)	Folyamatok (Hogyan?)	Helyszínek (Hol?)	Emberek (Ki?)	Idő (Mikor?)	Motiváció (Miért?)
Szervezeti vetület (Összefüggések rétege)	Mi a rendszer típusa, mi a terméke? A cég védendő értékei: jó hírnév védelme, a védendő információk	Hogyan működik? A védendő Szervezeti folyamatok (tranzakciók, kommunikáció)	Hol működik? Zárt rendszer, több telephely, külső partnerek, nyílt, országos /nemzetközi kapcsolatok	Ki használja? Szervezeti és menedzselési kérdések, ellátási lánc, stratégia partnerek, kiszervezés/szolgáltatás kihelyezés	Mikor használja? Határidők, ciklusok, azonnali igények, terhelés megoszlás, csúcsok	Miért használja? Szervezeti célok, sikertényezők, működési kockázatok
Szervezeti architektúra vetület (Koncepciók rétege)	Mit kell megvédeni? Szervezeti titok, szervezeti egységek, kapcsolataik	Hogyan működjön a védelem? Felső szintű biztonsági stratégiák: PKI, alkalmazás védelem	Hol vannak a védendő területek? A védelem helyfüggősége, biztonsági tartományok	Ki menedzsel? Menedzselés szervezeti modellje: biztonsági hatóságok, PCA, CA, RA	Mikor kell a védelem? Időpont, tartam? Jelszó, tanúsítvány élet-ciklus, CLR idő	Miért fontos? Szervezeti kockázat elemzés, sebezhetőség és költségtakarékosság
Tervezői vetület (System engineering, Logikai réteg)	Védendő adat-entitások és kapcsolatuk, PKI tanúsítvány, CA	Biztonsági szolgáltatások: hitelesség, teljesség, letagadhatatlanság	Védelmi terület definiálása, biztonsági tartományok logikai, fizikai, stb.	A jogosultsági profilok: felhasználó, rendszer-gazda, auditor	A biztonsági folyamat ciklusa jogosultság, tanúsítvány kiadáskor	Biztonsági irányelvek követelményei, CPS, helyi biztonsági tartományok irányelvei.
Kivitelezői vetület (Fizikai réteg)	Védendő adatstruktúrák: üzenetek, táblák, elektronikus aláírások	A biztonsági mechanizmus: titkosítás, vírus védelem, AC szerverek	A biztonságtechnológiai infrastruktúra elemeinek helye	Biztonsági fel-használói interfészek képernyő formája	Az ellenőrzési rendszer működtetésének időrendje	Biztonsági szabályok, feltételek és tevékenységek
Integrációs vetület (Elemek rétege)	Adatmezők és címek részletes specifikációja	Termék és eszköz: hardver, szoftver és a vonatkozó szabványok	Számítógépes folyamatok, csomópontok címei és protokollok	Felhasználói azonosítók, kivételek és ACL-ek	Biztonsági tevékenységek időtartama és sorrendje	Biztonsági tevékenységek és intézkedések

Üzemeltetési vetület, réteg	Üzemeltetési biztonság: bizalmasság, teljesség, jogosultság, felhatalmazottság	Felhasználók és rendszerek biztonsági adminisztrációja, mentések,	Hálózatok és platformok biztonsága a szabványok alkalmazásával	Felhasználók, operátorok és adminisztrátorok támogatása	Biztonsági tevékenységek időbeosztás szerinti végzése	Az üzemeltetés folyamatosságának és biztonságának fenntartása

4 SZERVEZETI ARCHITEKTÚRA

A korábbi szakaszokban az *architektúra* kifejezés mögött meghúzódó különböző jelentésekkel találkozhattunk – jellemzően az informatikai alkalmazásokkal és rendszerekkel kapcsolatban. Az *architektúra* kifejezésnek több mellékjelentése van a szervezeti stratégia szintjén. Az általános architektúra tervezési elvek alkalmazhatók az informatika olyan felépítése és kialakítása céljára, amely a *szervezeti*, üzleti *stratégiához* történő *illeszkedést* valósítja meg.

Szervezeti (vállalati) informatikai architektúra

- **Szervezeti (vállalati) informatikai architektúra**:Azoknak a stratégiai és architekturális tervezési elveknek a gyűjteménye, amely magában foglalja az **információ**, **szervezeti (vállalati) információrendszer** és a **műszaki, informatikai architektúrát**.

Az **információrendszer vagy informatikai stratégiai tervezés (IS/IST Strategic Planning, ISSP)** és a *szervezeti informatikai architektúra* tervezés bensőséges kapcsolatban áll egymással. A szervezeti informatikai architektúra készítés sok területen segíteni tudja a stratégiai tervezést, az informatikai fejlesztések, a projekt portfolió alapjait tudja megteremteni. *Szervezeti architektúra* (Ld.[34]) két formában jelenik meg, egyrészt az informatikai stratégiai tervezés folyamatának kísérője, másrészt mint egy élő organizmus, amelyik ésszerű módon alkalmazkodik a környezetéhez. Az informatikai stratégiai tervezés fekteti le a ciklikus szervezeti architektúra tervezés alapelveit. Az *információ*, a *szervezeti* és a *műszaki*, *informatika architektúra* az informatikai környezet és annak irányítási folyamatainak egészén átívelő, a részek közötti együttműködést megteremtő szinten létezik, és ezek az architektúra szintek kölcsönösen támogatják egymást. Az **alkalmazási (szoftver) architektúra** akkor lép működésbe, amikor egy egyedi információrendszer beszerzéséről vagy kifejlesztéséről van szó.

4.1 Információ architektúra

Az információ architektúra nézőpont a szervezet által végzett tevékenységekkel és a tevékenységekhez szükséges információk értelmében ragadható meg. Az adatok és tevékenységek magas szintű nézete teremti meg a szervezeti szintű követelményelemzés alapjait a szervezeti (vállalati) információrendszer architektúra kialakítása során.

Információ architektúra

- **Információ architektúra**: A szervezet által igényelt és használatban lévő információ szerkezete.

Az *információ architektúra* kialakításával kapcsolatos leglényegesebb tevékenységek:

- *A szervezet információ szükségleteinek feltárása*. A legfontosabb szervezeti (vállalati, üzleti) tények, adatok felismerése és ezeknek megfogalmazása a szervezet (vállalati, üzleti) információ szükségleteinek formájában.
- *Az információ architektúra meghatározása*. Az architektúra meghatározása a következő módszereket használja: párhuzamos lebontás (dekompozíció), értéklánc elemzés, és eseményelemzés.
- *A funkciók közötti függőségek elemzése*. A funkciók részekre bontása (dekompozíció) érvényességének ellenőrzése, továbbfinomítása, és a függőségek feltárása.
- *Az entitások és köztük fennálló kapcsolatok meghatározása*. Az információ architektúra adat oldalát pontosítja – lényegében ez egy szervezeti szintű adatmodellezési tevékenység.
- *Az információ szükségletek leképezése*. Az entitás típusok teljes listáján szereplő elemek és a feltárt információ szükségletek listáján szereplő elemek összerendelése.
- *Az entitás típusok használatának elemzése*. A szervezeti (vállalati, üzleti) funkciók által az entitás típusokon kiváltott hatások feltárása, helyességének ellenőrzése, a tevékenység hierarchia és entitás kapcsolat diagram tovább finomítása, pontosítása.
- *A szervezeti funkciók és az entitás típusok leképezése a szervezeti egységekre*. A szervezeti egységek és az adatok összekapcsolása, a szervezeti tevékenység hierarchia elemzésével és annak feltárásával, hogy az *információ architektúra* hogyan használja az adatelemeket.

4.2 Szervezeti (vállalati, üzleti) információrendszer architektúra

Szervezeti (vállalati, üzleti) *információrendszer architektúra* leírja szervezeti (vállalati, üzleti) információrendszereket és azokat az információkat, amelyeket a rendszerek elsődlegesen tárolnak az *információ architektúra* támogatása érdekében. *Szervezeti* (vállalati, üzleti) *infor-*

mációrendszer architektúra tudja jelezni a kezdetekben, hogy vajon a jelenlegi rendszerek (gyakran megörökölt, elavult vagy régi rendszerek – **legacy systems**) újra hasznosítására, továbbfejlesztésére, illetve új szervezeti (vállalati, üzleti) információrendszerek kifejlesztésére van szükség. *Szervezeti* (vállalati, üzleti) *információrendszer architektúra* kialakítása vezérli általában a jelenlegi információrendszerek és a szervezeti tevékenységek, a szervezeti információrendszerek és a kapcsolófelületek közötti összerendelést. A szervezet és az informatika irányítása szempontjából a *szervezeti* (vállalati, üzleti) *információrendszer architektúra* adja meg azt a környezet, amelyben az új rendszerek kialakítására irányuló kezdeményezések mérlegelhetők.

Szervezeti (vállalati, üzleti) információrendszer architektúra

Szervezeti (vállalati, üzleti) információrendszer architektúra: A szervezet összes információrendszerének struktúráját és tartalmát (információ és funkció értelmében) definiálja.

4.3 Műszaki, informatikai architektúra

A *műszaki, informatikai architektúra* elsősorban azt a **platformot** írja le, amely *szervezeti* (vállalati, üzleti) *információrendszer architektúra* és az *információ architektúra* támogatásához szükséges hardver, szoftver és infrastruktúra elemeket tartalmazza. Ezen kívül a *műszaki, informatikai architektúra* a *platform* elemeinek integritását, összhangját tartja fenn. Az információ-technológia megoldások kivitelezése, a műszaki, technológiai környezet tervezése, az információ-technológia világának változására adandó reagálások nagy mértékben függnek *műszaki, informatikai architektúra* definíciójától. A *műszaki, informatikai architektúra* kialakítása nemcsak azért felelős, hogy a technológiai környezet korrekt módon működjön, hanem a működéshez szükséges funkciók struktúráját is meghatározza.

A platform

A **platform**: Az architektúra központi fogalma a platform, amely a szervezet stratégiai vagyona. A platform magában foglalja az architektúrában definiált összes olyan kulcs fontosságú szolgáltatást, amely rendelkezésre áll az egyes szervezeti (vállalati, üzleti) információrendszerek számára az infrastruktúrán belül.

4.4 Az alkalmazási architektúra

Az *alkalmazási architektúra* az egyes alkalmazásokkal és rendszerekkel foglalkozik. Természetesen átfedés van általában a *műszaki, informatikai architektúra* és az *alkalmazási archi-*

tektúra között. A műszaki, informatikai architektúra a szabványokkal, technikákkal és az alkalmazási architektúra szabályozási és irányelvekkel kapcsolatos oldalaival foglalkozik. Az alkalmazási architektúra koncepcionális megalapozását és keretrendszereit a műszaki, informatikai architektúra szolgáltatja.

Alkalmazási architektúra

Alkalmazási architektúra:A szoftver rendszer szerkezetére, szervezésére vonatkozó lényeges döntések halmaza, valamint azoknak az architektúra tervezési elveknek a gyűjteménye, amely irányítja a szoftver szerkezet kialakítását.

5. Táblázat A jelentősebb architektúra megközelítések és szintjeik

Architektúra rétegek	Számítógép architektúra	OSI modell Hálózati szoftver architektúra	Elosztott rendszerek architektúrája	Szervezeti (vállalati) architektúra
0. szint	Digitális logika	Fizikai	Fizikai réteg / hardvererőforrások	Műszaki, informatikai, technológiai architektúra (hardver, szoftver, ICT kommunikáció)
1. szint	Mikro-architektúra	Adatkapcsolati réteg		
2. szint	Utasításrendszer architektúra	Hálózati réteg		
3. szint	Operációs rendszer	Szállítási réteg	Operációs rendszer	Alkalmazási rendszer (szoftver) architektúra
4. szint	Assembly	Viszony réteg (Session)	Hálózati réteg	Információrendszer architektúra
5. szint	Magas szintű programozási nyelvek	Megjelenítési réteg	Köztes réteg (Middleware)	Információ architektúra
6. szint		Alkalmazási réteg	Alkalmazási réteg	Szervezeti (vállalati, üzleti) architektúra

A *szervezeti (vállalati, üzleti) architektúrával* kapcsolatos tevékenység a szervezet átalakítás, transzformáció *irányítása* részének tekinthető.

4.5 Zachman féle szervezeti architektúra keretrendszer (The Zachman Enterprise Framework)

A keretrendszer valójában egy olyan **ontológia** a szervezeti architektúra leírására, fejlesztésére, amely az idők folyamán (pontosan 1987 óta, [44]) komoly evolúción ment keresztül. A keretrendszer nem módszertan, mivel nem ad folyamat leírást, előírást a szervezeti architektúra kialakítására, hanem egy deklaratív leírása a szervezetnek (vállalatnak, üzletnek), egy struktúra a szervezeti (vállalati, üzleti) információrendszerek fejlesztésére. A későbbiekben több szervezet, több iparágban– a szerzők és a keretrendszer eredeti szándékai szerint - egy szervezeti szintű architektúra szemléletben a szervezetek folyamatainak fejlesztésére, javítására kezdték el széles körben használni. A keretrendszer tehát nem módszer, nem módszertan, nem tartalmaz architektúra kialakítására lépéseket, technikákat, nyelveket és folyamat leírást, folyamat-központú megközelítést. (Ld. [75]). Más informatikai terminológiát használva: **meta-modellként** szolgál, a *szervezeti (vállalati, üzleti) architektúra* kialakításához.

4.5.1 A keretrendszer oszlopainak jelentése

A szervezeti (vállalati, üzleti) architektúra kertrendszer elemeit, egy két-dimenziós mátrixban, táblázatban adta meg Zachman. A táblázat oszlopainak megfelelő első dimenzió elemei, a vizsgált dolog egy-egy oldalának („*aspect*") felelnek meg. Rudyard Kipling egy versében ezt a hat kérdést „ A hat derék szolgaként" fogalmazta meg[3]. Az oszlopok fejlécében a következő kérdések találhatóak: **Mit**?, **Hogyan**?, **Hol**?, **Ki**?, **Mikor**? és **Miért**?. (Ld.**9. ábra**). A másik dimenzió, a táblázat sorainak megfelelő dimenzió, bizonyos szempontokat, perspektívát („*perspective*"), a keretrendszer egy-egy nézőpontját testesíti meg. Nevezetesen a következőket: a **szervezeti (vállalati, üzleti) tervező** („*planner*"), a **tulajdonos** („*owner*"), a **tervező** („*designer*"), a **kivitelező / építő** („builder"), **alvállalkozó / beszállító, készítő** („*subcontractor*"), és végül a **működő szervezet** („functioning enterprise").

A Zachman féle keretrendszer általános ábrázolása egy 6x6-os mátrix, aminek oszlopait a kérdések és sorait a nézőpontok határozzák meg. A keretrendszer elemeinek ábrázolása a táblázat celláival történik, amik a kérdő szavak és a nézőpontok metszéspontjai.

Amióta John A. Zachman publikálta módszertanát, azóta az épületek, repülőgépek, és más komplex ipari termékek leíró ábrázolásának, architektúrájának meta-modellezéséhez is felhasználják ezt a megközelítést. Ez bizonyítéka a Zachman féle keretrendszer létjogosultságának.

A keretrendszer segítséget ad a szervezet céljainak, működésének feltételeinek, környezetének vizsgálatára, a szervezet és az informatikai funkció vezetési szintjein elhelyezkedő vezetőkkel, kezdve a felső vezetéssel a stratégiai szinten.

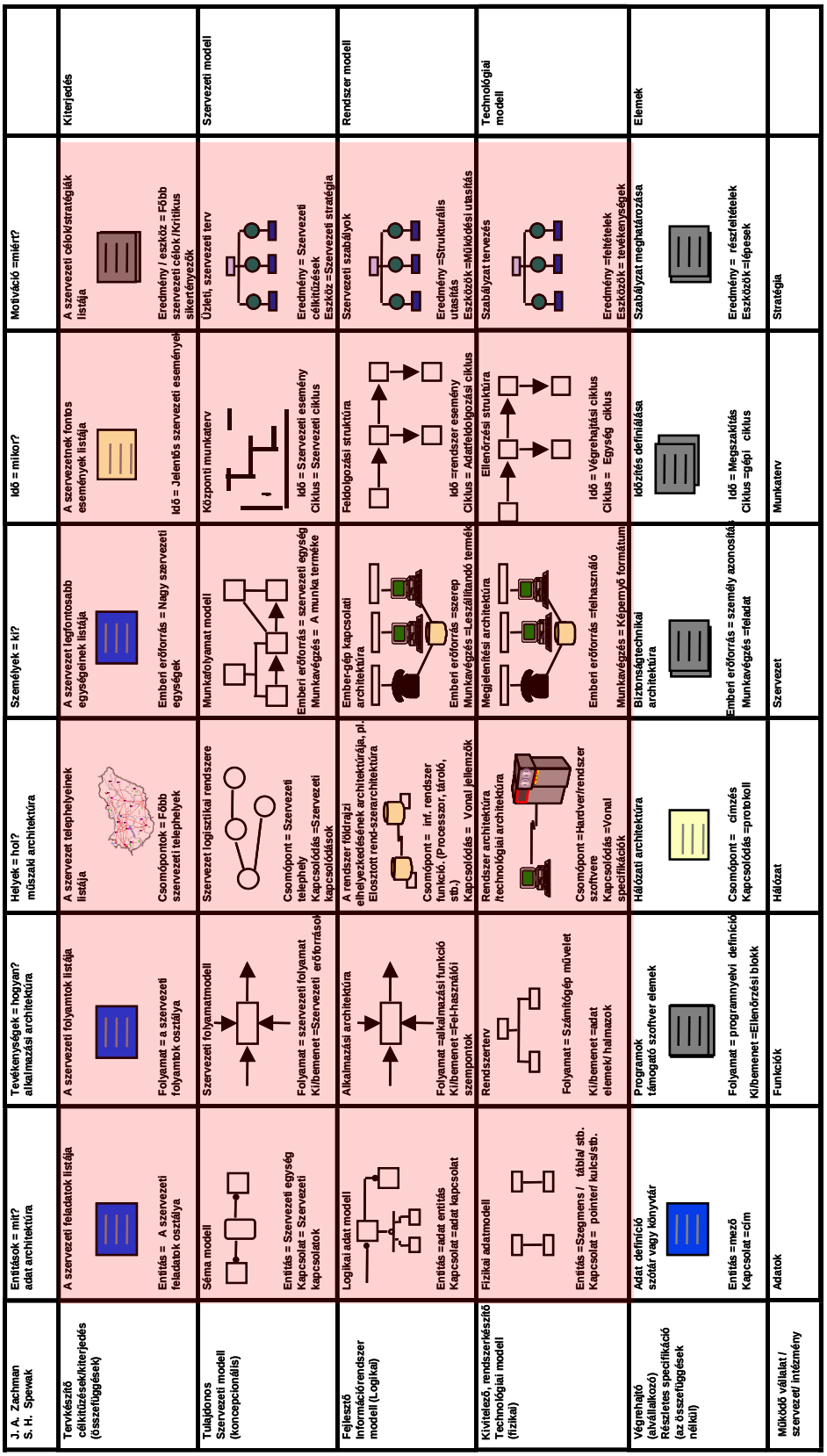
1. oszlop: **Adat (***mit***)** : Ez az oszlop a szervezet (vállalat, üzlet) működéséhez szükséges adatokkal foglalkozik, az adatok szerkezetével, hogyan tárolják az adatokat stb.
2. oszlop **Funkció** (*hogyan*): Ez az oszlop a szervezet (vállalat, üzlet) működésével foglalkozik. A szervezet stratégiai célkitűzéseit, „küldetését" fordítja le a szervezeti működés egyre részletesebb leírásaira.
3. oszlop **Hálózat** (*hol*): Ez az oszlop a szervezet (vállalat, üzlet) elemeinek, tevékenységeinek földrajzi elhelyezkedésével, szétosztottságával foglalkozik.
4. oszlop **Személyek** (*ki*): Ebben az oszlopban a szervezetben munkát végzőkkel, a munkafeladatok személyekhez rendelésével, az emberek közötti kapcsolatokkal foglalkoznak.
5. oszlop **Idő** (*mikor*): A valóságos idő egy absztrakciójával foglalkozik azért, hogy az események közötti kapcsolatokat meg lehessen tervezni, amelyek meghatározzák a teljesítmény kritériumokat és számszerűsíthető szolgáltatási szinteket szabnak meg a szervezet erőforrásai tekintetében.
6. oszlop **Motiváció** (*miért*): A szervezet (vállalat, üzlet) motivációjának meghatározásával leíró formában foglalkozik, és általában célok és elérésükhöz szükséges eszközök megfogalmazásán keresztül jeleníti meg a szervezet motivációit. Az eszközök itt általában a cél eléréséhez használt módszert jelentik.

4.5.2 A keretrendszer sorainak jelentése:

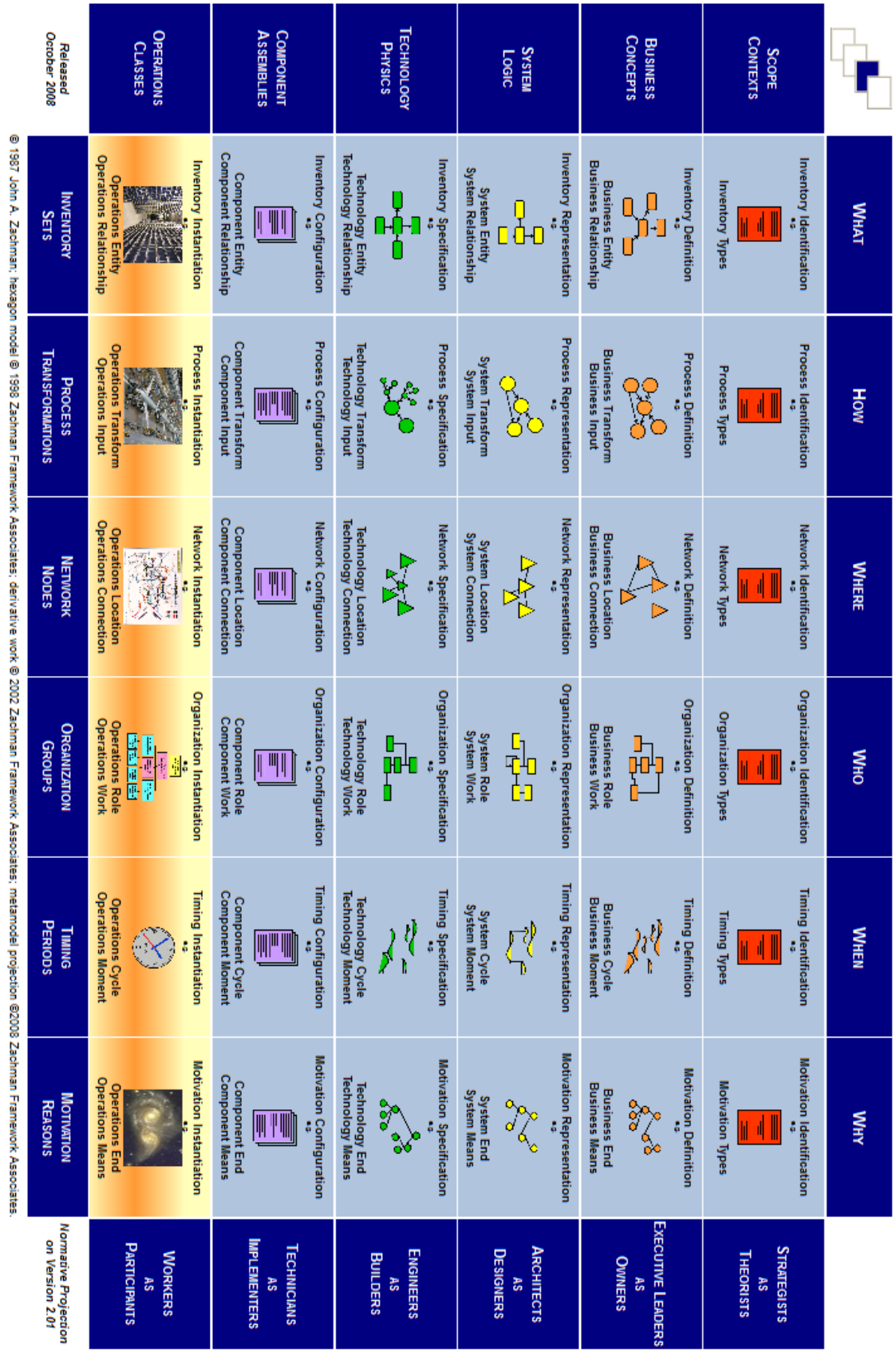
1. sor: **Kiterjedés, terjedelem** : Az első architektúra vázlatot jelenti, amely egy olyan „gombócokat" tartalmazó ábra, amely nagyvonalakban leírja az elképzelt végső struktúrának a kiterjedését, határait, nagyságát, körvonalait, térbeli kapcsolatrendszerét és alapvető céljait. Tulajdonképpen egy *szervezeti (vállalati, üzleti) tervező* vagy **befektető** számára szóló vezetői összefoglalónak felel meg, akinek a leendő rendszer kiterjedéséről, a várható költségekről és a nyújtandó szolgáltatásokról kellene egy előzetes képet kapnia.
2. sor: **Szervezeti (vállalati) modell :** A következő ábrázolás, az architektúra tervezőé, aki a rendszer végső felépítését annak a tulajdonosnak a szemszögéből, perspektívájából írja le, akinek majd naponta együtt kell élnie ezzel a szervezeti (vállalati, üzleti) környe-

zettel. Megfelel a szervezeti (vállalati, üzleti) modellnek, amely a szervezeti (vállalati, üzleti) működés tervét testesíti meg és a legfontosabb szervezeti (vállalati, üzleti) egységeket, elemeket, folyamatokat és köztük fennálló kölcsönhatásokat jeleníti meg.

3. sor: **Rendszer modell**: Ez az architektúra tervkészítő tervezete, amely az eddigi modell ábrázolásokat lefordítja a rendszertervező szemszögének, perspektívájának megfelelő részletes műszaki leírásokra, specifikációkra.
4. sor: **Technológia modell**: (műszaki, informatikai modell) A szállítónak általában az architektúra tervkészítő tervezetét át kell dolgoznia azért, hogy a kivitelező szemszögéből, perspektívájából értelmezhető legyen, visszatükrözze azokat a korlátokat és peremfeltételeket, amelyek a rendelkezésre álló eszközökből, technológiákból, műszaki lehetőségekből, anyagokból állnak. A kivitelező (rendszerkészítő) tervezete a technológiai modellnek felel meg, amelynek a feladata az , hogy az információrendszer modellt a programozási nyelvek, a számítógép perifériák és más technológiai elemekhez illeszsze, adaptálja.
5. sor: **Részletes specifikáció**: Ez a modell megfelel annak a részletes specifikációnak, amelyet azoknak a programozóknak adnak át, akik egyes egyedi modulok programozását végzik el tekintet nélkül arra a környezetre illetve annak szerkezetére, amiben dolgoznak, és / vagy a folyamat tervezők kapják meg ezeket a terveket azért, hogy a munkafolyamatok részletes tervét elkészítsék. (a rendszer tényleges megvalósítása, telepítés, üzembe helyezés).
6. sor: **Működő szervezet** (vállalat) : Végül, a rendszert elkészítik és a szervezet részévé válik. Ebből a szemszögből a program listák, az adatbázis specifikációk, a hálózatok és így tovább jelennek meg, amelyek mindegyike egy bizonyos rendszert alkot. Ezeket a leírásokat az adott rendszerhez illeszkedő, specifikus műszaki, informatikai terminológiával írják le.



8. ábra Szervezeti (üzleti vállalkozás) architektúra Zachman és TOGAF keretrendszere. A TOGAF a színezett részt fedi le.



9. ábra The Zachman Framework²™ Standards, 2008[4]

5 INFORMÁCIÓ BIZTONSÁGI ARCHITEKTÚRA (INFORMATION SECURITY ARCHITECTURE)

A hálózati biztonsági követelmények teljesítéséhez jelentős mértékben hozzájárulnak a három A-val jelzett eljárások összetevői, az *autentikáció (authentication)*, magyarul a **hitelesség vizsgálat**, hitelesítés, *autorizáció (authorization))*, magyarul **jogosultságok megadása**, engedélyezése, azaz a felhasználói jog megadása, és *accounting*, a **felhasználói tevékenységek** nyilvántartása.

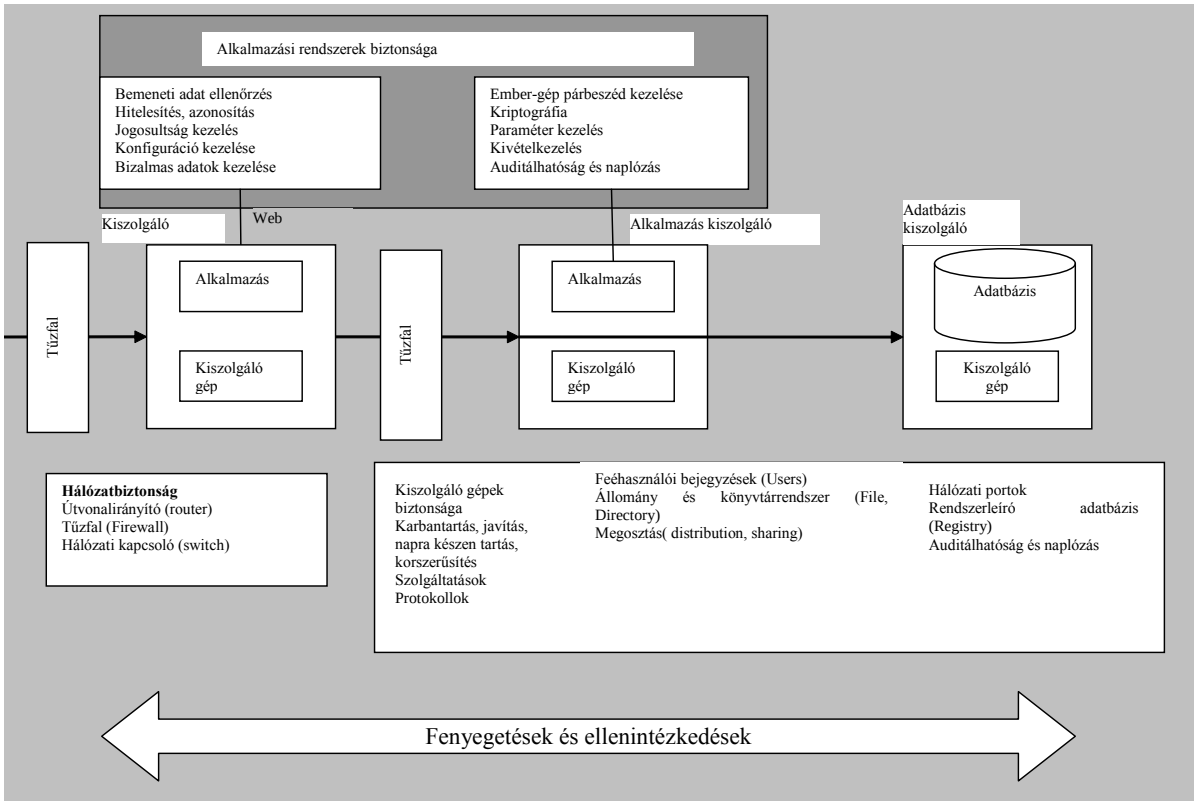
Az *elektronikus autentikáció*, hitelesítés az a folyamat, amely során egy számítógépet vagy hálózati felhasználót hitelt érdemlően igazolnak, így lényegében különbözik attól, amit jogosultságvizsgálatnak nevezünk, amelyre az egyszerű, jelszavas azonosítást alkalmazzák. A tényleges hitelesítés biztosítja, hogy az adott személy valójában az akinek állítja magát. A hitelesítés (autentikáció) különbözik az azonosítástól, amely azt határozza meg, hogy az adott személyt a rendszer nyilvántartja-e, és különbözik az autorizációtól, amely az Hitelesített személyazonosság alapján feljogosítja a felhasználót bizonyos speciális rendszer erőforrások elérésére.

Az **Autentikációt**, **Autorizációt** és **Accounting**-ot együttesen megvalósító rendszert nevezik „AAA" rendszernek. A biztonsági megoldások, mint az „AAA" szolgáltatás, *tűzfalak*, titkosítás, *behatolás figyelés*, az *aktív auditálás*, a *szolgáltatásminőség biztosítása*, magasabb prioritást kapnak a rendszerekben. A hozzáférés ellenőrzési lista (ACL), a ponttól-pontig protokoll szerinti jelszavak és az „AAA" szerverek alkalmazása megfelelő megoldást biztosítanak a központi alkalmazások, adatbázisok és a különböző helyszínen azokat elérni kívánó alkalmazások közötti kapcsolattartásra.

A biztonsági megoldások az alábbi három csoportba sorolhatók:

- **Azonosság:** Ki az, akinek megengedett arról a helyről valamit csinálni? A biztonságos autentikáció, autorizáció és accounting szerver, és a közigazgatási CA (Certificat Authority) nyújtják ezt.
- **Sérthetetlenség.** Az információt és az erőforrásokat a jogosulatlan hozzáféréstől védi tűzfalakkal, hozzáférési ellenőrzési listákkal (ACL), és titkosítással, azért, hogy az adatokban, információkban jogosulatlan, szándékos és szándéktalan károkozás ne valósulhasson meg..

- **Aktív audit.** Figyeli a hálózati forgalmat, azonosítja a biztonsági kockázatokat, érvényesíti a biztonsági koncepciót és semlegesíti a jogosulatlan tevékenységet egy valósidejű behatolás érzékelővel és egy proaktív sebezhetőség felderítővel.



10. ábra Biztonsági architektúra

AAA, Authentication, Authorization, Accounting/Access Control

Az **AAA rendszer** egy keret rendszer, mely három egymástól független biztonsági funkciót valósít meg. Ezen funkciók a következők:

- *Authentication* - a felhasználó azonosítása, hitelesítése mielőtt hozzáférne bármely erőforráshoz, szolgáltatáshoz a hálózatban.
- *Authorization* - ez a funkció határozza meg, hogy felhasználó milyen erőforrásokhoz, szolgáltatásokhoz férhet hozzá a hálózaton.
- *Accounting* - E funkció segítségével lehet nyomon követni, hogy egy felhasználó milyen hálózati erőforrásokat, szolgáltatásokat vett igénybe.

Az *AAA* rendszerek a ***RADIUS*** és a ***TACACS+*** *protokollokat* használják kommunikációs célokra. Követelmény az AAA rendszerrel szemben:

- **Központosított menedzsment**. Valamennyi felhasználó adatai egy központi adatbázisban legyenek tárolva.

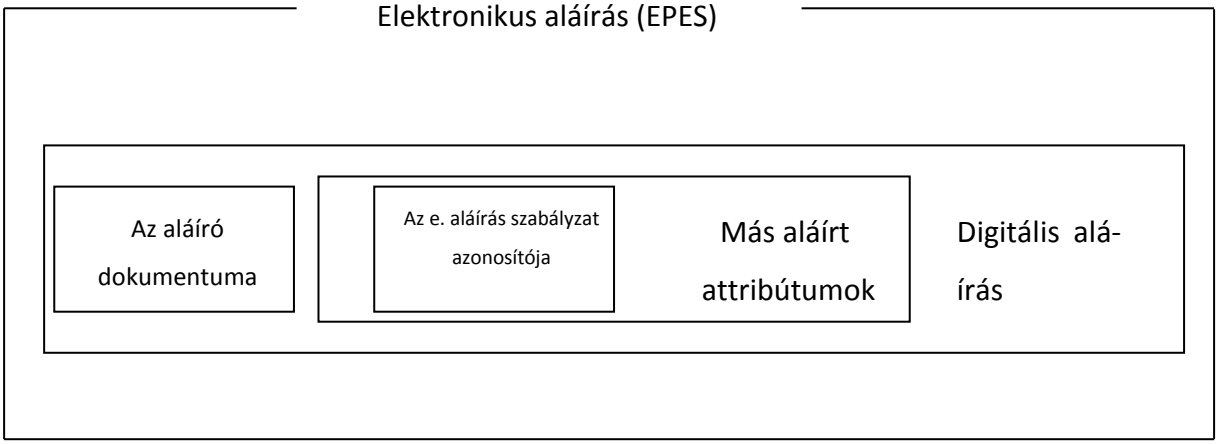
- **Skálázhatóság**. Külső adatbázis szerver használatával akár nagy mennyiségű felhasználó kezelésére is legyen alkalmas.
- Szabványos protokoll az AAA szerver és a „Network Access Server”-ek (a hálózat elérhetőségéről gondoskodó kiszolgáló gépek) között.
- **Fexibilitás**, egyszerű kezelhetőség. Felhasználói csoportok definiálásával az adminisztrációs munka jelentősen csökkenthető legyen.

5.1 PKI (Publikus Kulcsú Infrastruktúra) szolgáltatások és jellemzőik

A PKI szolgáltatásai végfelhasználókat **tanúsítványokkal** (certification) látja el, amelyek a kulcspárok nyilvános kulcsát és azonosító adatait tartalmazó digitális tanúsítványok. A magánkulcsok védett tárolására és a kriptográfiai műveletek biztonságos végrehajtására mikroszámítógépet is tartalmazó kriptográfiai eszközt (intelligens kártyát, USB tokent vagy SIM kártyát) alkalmaz az infrastruktúra. A kevésbé védhető személyi számítógépes, illetve szoftveres megoldások is elterjedtek (a számítógépek merevlemezes tárolói önmagukban nem biztosítanak kellő védelmet a kulcsok tulajdonos tudtán kívüli ellopása, letöltése, kompromittálása ellen)[5]. A tároló megnyitásához, illetve a kulcsok, műveletek aktiváláshoz PIN kód vagy jelszó szükséges.

A felhasználói és alkalmazási követelmények kielégítése, a bizalom megerősítése céljából a PKI az informatikai biztonság fogalomkörében az alábbi szolgáltatásokat jelenti:

- **Azonosítás** (*autentikáció*, vagy néhol *hitelesítés*) során hitelt érdemlő módon ellenőrizhető, hogy a kérdéses végfelhasználó az-e, akinek a személyazonosítás (identification) során mondta magát. A PKI lehetőséget nyújt a „valamit tud (PIN), valaminek a birtokában van (magán kulcs), valami egyedi jellemzővel rendelkezik (ujjlenyomat)" együttes alkalmazására, az un. szigorú azonosításra, amikor is az igénybe vett jellemzők száma szerint kettő-, illetve háromtényezős azonosításról beszélünk. Az azonosítás különböző jellemzők, attribútumok alapján nemcsak személyek, hanem számítógépek, más hálózati eszközök, elektronikus okmányok, dokumentumok esetben is szükséges és lehetséges a digitális tanúsítványok felhasználásával.



11 ábra A fokozott szintű elektronikus aláírás követelményeinek megfelelő aláírás szerkezete a ETSI szabvány szerint

- Az információ **sértetlenség**ét, **épségét**, teljességét (az angol megnevezésből eredően integritásnak is mondják) a PKI digitális aláírás szolgáltatása oly mértékben biztosítja, hogy az eredetitől való egyetlen karakter eltérését is jelzi. Bárki, bármikor ellenőrizni képes, hogy egy digitálisan aláírt elektronikus dokumentumot utólag nem módosítottak-e, azonos-e az aláírás kori állapotával. A *digitális* és az *elektronikus aláírás* egymással nem felcserélhető eljárás. Viszonyukat a 11 ábra szemlélteti az ETSI CAdES szabvány alapján. A hitelesség megőrzése azonban csak a PKI más szolgáltatásaival együttesen biztosítható. Az elektronikus események (okirat aláírása, tranzakció, üzenet küldése, vétele) **letagadhatatlanság**át megbízható harmadik fél bevonásával lehet biztosítani. A *letagadhatatlanságot* az elektronikus aláírás önmagában csak olyan értelemben biztosítja, hogy a tanúsítványt birtokló és a használatához szükséges PIN kódok vagy jelszavak ismerője lehetett az üzenet küldő (alapfeltételezés az, hogy ez megegyezik azzal a személlyel, akinek a tanúsítványt kiállították). Ennek legelterjedtebb formája az **időbélyeg**-szolgáltató igénybevétele egyik, vagy mindkét fél részéről. Önmagában az időbélyeg csak azt igazolja hiteles módon, hogy az elektronikusan aláírt dokumentum az időbélyeg-

zés pillanatában már létezett.

- Az elektronikus üzenetek, dokumentumok **bizalmasság**át (az eljárást elterjedten titkosításnak, helyesebben rejtjelezésnek, algoritmikus, *kriptográfiai védelemnek*, információ védelemnek kell nevezni, esetleg titkosírásnak nevezik) - azaz, hogy jogosulatlan ne ismerhesse meg az információt - a nyilvános kulcsú kriptográfia egyszerűen kezelhető módon biztosítja. A megfelelő tanúsítvány ismeretében az üzenet címzettje részére bárki nyílt hálózaton is oly módon küldheti el elektronikus üzenetét, hogy annak tartalmához - például adóbevallása, szolgálati, üzleti titkai, magánélete, személyes adatai védelmében - csak a címzett férhessen hozzá. A PKI technológia hasonló módon alkalmas a végpont-végpont közötti elektronikus kommunikáció védelmére, illetve egyes zárt csoportok, a végfelhasználók adatainak, fájljainak védelmére. (pl. a notebook-okon tárolt adatok esetén.)

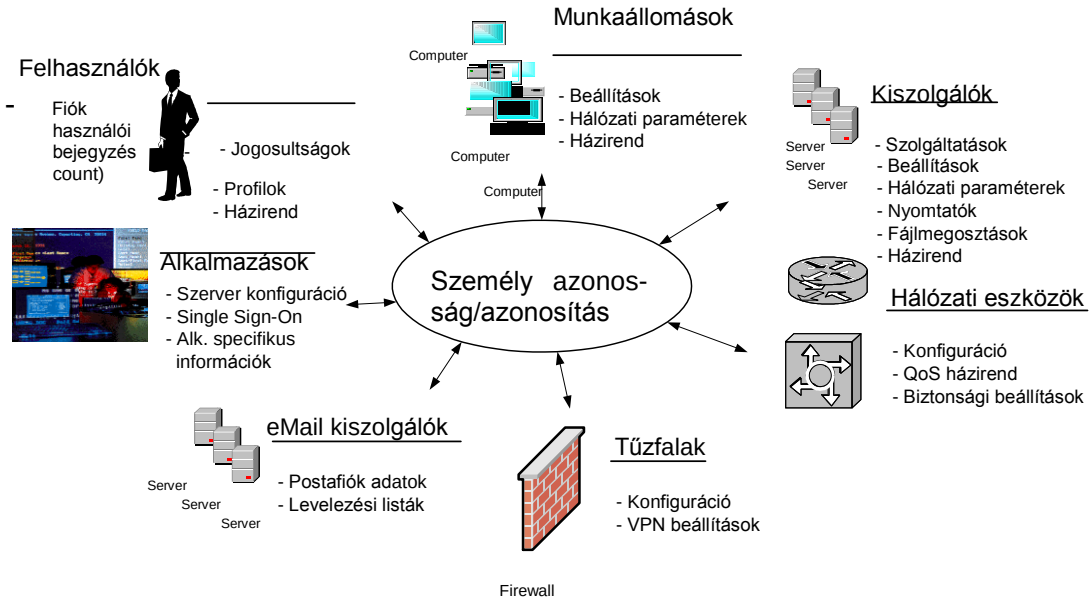
12. ábra A nyilvános kulcsú (PKI) infrastruktúra elemei

Személy azonosításra szolgáló tanúsítvány **fokozott** biztonságú vagy **minősített** elektronikus *személy azonosításra* alkalmas tanúsítványt tartalmaz, amely a kártya megszemélyesítésekor kerül a kártyára.

6. Táblázat Tanúsítványokkal és elektronikus aláírással kapcsolatos fogalmak

Tanúsítvány	A hitelesítés-szolgáltató által kibocsátott igazolás, amely az ***aláírás-ellenőrző adatot*** egy ***meghatározott személyhez*** kapcsolja, és igazolja e személy *személyazonosságát* vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget (Magyarországon törvény szabályozza, az „**Elektronikus aláírás törvény**”, *Eat*. 9. § (3), illetőleg (4) bekezdése szerin)[6]
Minősített tanúsítvány	Az *Eat*. 2. számú mellékletében foglalt követelményeknek megfelelő olyan tanúsítvány, melyet minősített szolgáltató bocsátott ki
Fokozott biztonságú elektronikus aláírás	Olyan elektronikus aláírás, amely 1. alkalmas az aláíró azonosítására, 2. kizárólag az aláíróhoz köthető, 3. olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak, és 4. a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően a dokumentumon végzett - módosítás érzékelhető
Minősített elektronikus aláírás	Olyan - fokozott biztonságú - elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki
Minősített hitelesítés-szolgáltató	Az *Eat*. szerint nyilvántartásba vett, minősített tanúsítványt a nyilvánosság számára kibocsátó hitelesítés-szolgáltató
Elektronikus aláírás	Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat
Elektronikus aláírás hitelesítés-szolgáltató	Az elektronikus aláírást igénylő személyét azonosító, tanúsítványt kibocsátó, nyilvántartó szervezet
Elektronikus aláírást létrehozó	Az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult, valamint az a jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet, amely az aláírás-létrehozó eszközt birtokolja, és akinek a nevében az őt képviselő természetes személy az elektronikus aláírást az elektronikus dokumentumon elhelyezi, valamint aki meghatározza, hogy a nevében jogszabályban meghatározott feltételeknek megfelelő informatikai eszköz elektronikus aláírást elektronikusan dokumen-

	tumon elhelyezzen
Elektronikus aláírás felhasználása	Elektronikus adat elektronikus aláírással történő ellátása, illetve elektronikus aláírás ellenőrzése
Elektronikusan történő aláírás	Elektronikus aláírás hozzárendelése, illetve logikailag való hozzákapcsolása az elektronikus adathoz
Elektronikus aláírás érvényesítése	Annak tanúsítása minősített elektronikus aláírás vagy e szolgáltatás tekintetében minősített szolgáltató által kibocsátott időbélyegző elhelyezésével, hogy az elektronikus dokumentumon elhelyezett elektronikus aláírás vagy időbélyegző, illetve az azokhoz kapcsolódó tanúsítvány az időbélyegző elhelyezésének időpontjában érvényes volt



13.ábra Személy azonosítás logikai/technológiai architektúra komponensek

5.2 Tanúsítvány alapú személyi azonosítás

Az azonosság megállapításához a hardver és/vagy szoftver eszköz **azonosításra alkalmas tanúsítványt (**nem elektronikus aláírást és nem titkosírásra alkalmas tanúsítványt**)** tartalmaz.

- *Fokozott biztonságú elektronikus* személy *azonosításra* alkalmas tanúsítvány a kártya/adathordozó megszemélyesítésekor kerül a kártyára.

- *Minősített elektronikus* személy *azonosításra* alkalmas tanúsítvány a kártya megszemélyesítésekor kerül a kártyára. A tanúsítvány elektronikus aláírási tranzakcióban történő aktiválásához jelszó/PIN (*jel kifejezés*) kód szükséges.
- A *minősített elektronikus aláírásra* szolgáló tanúsítvány az, amely a törvény ereje folytán automatikusan egyenértékű a papír alapú dokumentációval, és kézzel aláírt iratokkal, okiratokkal.[7]

5.3 Időpecsét (időbélyeg) szolgáltatás

A letagadhatatlanság alátámasztására időpecsét szolgáltatást kell/lehet igénybe venni.
Ezzel a megoldással, az egyes személy-azonosító tanúsítvány (kártya) *tranzakcióknál* az eszköz tanúsítványok segítségével, az időpecsét szolgáltató időpontjával és magánkulcsával alkalmas bináris lenyomat készíthető, amely a letagadhatatlanságot egy adott időponthoz kötve tudja igazolni.

5.4 Biztonságos vonali kommunikáció által igényelt megoldások

A bizalmas (kényes) személyi és személyes adatok forgalma igényli a kommunikációs csatornák végpont-végpont algoritmikus, *kriptográfiai* védelmét.
A biztonságos vonali kommunikáció információvédelme érdekében a PKI szolgáltatások közül az eszköz tanúsítványok intenzív használatára mindenképpen szükség van.
A letagadhatatlanság egyik megoldásaként szóba jövő időpecsét szolgáltatáshoz is szükség van eszköz tanúsítványra:
Az ügyfél oldali eszközök (kártya terminál, PC) és a központi rendszerek kommunikációjának védelme a következő eszközökkel támogatható:

a. SSL csatorna (eszközök PKI tanúsítványára támaszkodva);
b. VPN alagút, végződtetés tűzfalon, vagy egy konkrét alkalmazási rendszeren, kiszolgáló gépen, a szóban forgó végpontok PKI tanúsítványára támaszkodva;
c. A küldött üzenetek titkosírása, kriptográfiai védelme, sifrírozása, rejtjelezése PKI tanúsítvány alapokon, rejtjelezési célokra kibocsátott tanúsítvány segítségével.

5.5 Kommunikációs és hálózatbiztonsági szempontok

Egy információbiztonságot támogató architektúra főbb elemei:

1. Kártyaterminál;
2. munkaállomás (PC);
3. Egyéb számítógép, informatikai eszköz (kiszolgáló gépek);
4. Alkalmazási/ szolgáltató rendszerek;
5. Telefonon (mobil, vezetékes), interneten végfelhasználók. (Itt elkerülhetetlenül alkalmazni kell a dinamikusan generált, korlátozott idáig érvényes titkos kód, a hitelesítés és viszontazonosítás céljára, ha olyan események fordulnak elő, amelyeknél fokozott biztonságú személyazonosításra és az azonosság hitelesítésére van szükség).
6. Világháló (Web/Internet) kapcsolat.

A kommunikáció és hálózati biztonság egy adott szintjének megvalósításához szükségesek az A-val jelzett eljárások és azok elemei, az *autentikáció*, magyarul a **hitelesség vizsgálat**, hitelesítés, *autorizáció*, magyarul **jogosultságok megadása**, engedélyezése, azaz a felhasználói jog megadása, és *accounting*, a **felhasználói tevékenységek** nyilvántartása. A személy vagy eszköz *hitelesítését* megelőzi az azonosítási (**identification**) eljárás.

A három „A” funkciót ellátó hálózatban a következő elemek találhatók:

- Távoli hálózati hozzáférést biztosító szerver vagy útvonal-irányító (NAS)
- Biztonsági hozzáférést kontrolláló szerver (ACS) és a hozzáférési lista (ACL)
- Token card szerver (ideiglenesen, rövid ideig érvényes jelszavak, kódok létrehozására) telefonos vagy internetes ügyfélszolgálat számára.
- Ellenőrző/irányító adminisztrátori munkaállomás,
- X.500, X.509, illetve LDAP címszolgálat
- Tanúsítvány kibocsátás és hitelesítési szolgáltatás)

A végponttól végpontig biztonságot nyújtó architektúra az alábbi elemeket tartalmazhatja:

- Intelligens hálózati eszközök, amelyek „alkalmazás biztosak”, azaz alkalmasak a rendszergazdai és rendszer felügyeleti utasításokat értelmezni és biztosítani a biztonsági ellenőrzési követelményeket, minden felhasználó, illetve alkalmazás esetére.
- Szolgáltatásminőség és biztonsági, üzemeltetési irányelvek (*’policy’*) szolgáltatásokhoz kiszolgáló alapú ellenőrzési mechanizmust nyújtó rendszerek, amelyek a rendszeradmi-

nisztrátor és a hálózat közötti kapcsolati felületről gondoskodnak. Fordítóprogramok automatizálják a hálózatra kapcsolt eszközök konfigurálást, a központi kezelőpultról és az üzemeltetési irányelveknek megfelelően optimalizálják a hálózatot. Intézik a biztonsági beállítások, a kulcsok hálózati telepítését az egyes elemekre.

- **Regisztrációs** és **címtár** (*directory*) szolgáltatások dinamikus kapcsolatot teremtenek az üzemeltetési irányelvek és a hálózati címek, felhasználói és alkalmazási profilok, valamint bizonsági irányelvek telepítése és érvényesítése szempontjából fontos információk között. Ezeknek a szolgáltatásoknak az alapja tartománynév szerver (DNS)/ dinamikus számítógép konfigurációs protokoll (DHCP) szerver rendszer és az LDAP (Lightweight Directory Access Protocol) alapú címtárak.

5.6 Biztonsági architektúra követelmények

A megrendelő, felhasználó által támasztható architektúra követelmények felsorolása:

1. Hozzáférés ellenőrzés, nyomon követés
2. Bizalmas (titkos) adatkezelés
3. Üzenetek épsége, sértetlensége (integritás)
4. A szoftver érintetlensége, sértetlensége (integritás)
5. Az adatok épsége, sértetlensége (integritás)
6. Letagadhatatlanság
7. Rendelkezésre állás
8. Költség
9. Teljesítmény
10. Használhatóság

A követelmények kielégítését különböző architektúra elemekkel lehet megoldani:

1. Felhasználói azonosító
2. Jelszó, titkos kifejezés, PIN kód
3. Magas biztonsági fokozatú intelligens kártya (eszköz) (COTS)
4. Biometriai olvasó (COTS)
5. Intelligens kártyaolvasó (COTS)
6. Kártyaolvasó (COTS)
7. Kizárólagosan kriptográfiai eljárásokra szánt hardver kiszolgáló gép (kulcsolás, visszafejtés)
8. Kriptográfiai eljárásokra, algoritmusokra szoftver (kulcsolás, visszafejtés)(COTS)
9. Időpecsét szolgáltatás
10. Kriptográfiailag védett üzenettovábbítás (sifrírozás, rejtjelezés, titkosírás)

11. Kriptográfiailag védett adatbázisrekord
12. Behatolás észlelő, védelmet nyújtó szoftver (Intrusion Detection/Protection Software) (COTS)
13. Vírusvédelmi szoftver (COTS)
14. Elektronikus/digitális aláírás
15. Egy jelszó, egyszeri alkalommal (Single Sign-On)
16. Fizikailag védett terem/helyiség a kiszolgáló gépeknek
17. Biztonsági őrök video kamerákkal

5.7 Web szolgáltatások biztonsági kérdései

A Web szolgáltatásokkal kapcsolatos szabványok és protokollok a Web szolgáltatásoknak csak a gerincét adják, azon túl még számos kiegészítésre és további részprobléma megoldására van szükség ahhoz, hogy az egész mechanizmus megbízhatóan működő rendszerré álljon össze. Az egyik terület a ***biztonság*** kérdése, nevezetesen a *hitelesítés* (*authentication*) és a *jogosultságok* megadása (*authorization*) problémája, továbbá a rendszer/szolgáltatás *hozzáférési jogosultságok* (*access control*) kezelése (AAA, ld. 5.1).

Az egyik leggyakoribb probléma, amivel a köztesszoftver protokollok szembenéznek az, hogy nem kifejezetten működnek jól az Interneten, mivel kapcsolatokat akadályozzák a tűzfalak. A legtöbb szervezet nem szeretné, ha az általuk használt protokollok kívülről is hozzáférhetővé válnának, ezért a belső rendszereket tűzfalakkal veszik körbe.

Egy gyakori megoldása ennek a problémának, melyet a Web szolgáltatások is alkalmaznak: a ***Web protokollok*** alkalmazása, mivel a HTTP-t mint transzport protokollt a legtöbb tűzfal átengedi. A HTTP protokoll ilyen jellegű alkalmazása kényelmes lehet, de ugyanakkor biztonsági fenyegetést is jelenthet, mivel a HTTP kapcsolatot már nem csak arra használjuk, hogy weboldalakat töltsünk le.

A *WS-Security (15, Erl 2005)* és a hozzá kapcsolódó szabványok azt tűzték ki célul, hogy ezeket a problémákat erős kriptográfiai módszerekkel küszöböljék ki. Ezt pedig a hívók azonosításával (autentikáció) és az információ védelmével (titkosítás) teszik meg, valamint biztosítják az információ integritását (épségét, sértetlenségét) (pl. digitális aláírással). Ezeket a szabványokat úgy alkották meg, hogy könnyedén kiterjeszthetőek és adaptálhatóak legyenek.

A Web szolgáltatás szabványok támogatják a tranzakciókat és megbízható üzenetküldést. A Web szolgáltatás tranzakciók két típusát támogatja a szabvány. A *WS- AtomicTranscations* a hagyományos elosztott ***ACID*** (Atomicity (atomicitás), Consistency (konzisztencia), Isolation

(izoláció), és Durability (tartósság)) tranzakciókat támogatja és bizonyos szintű biztonságot valamint gyors válaszidőt feltételez. Emiatt ez a módszer csak a belső integrációs feladatoknál alkalmazható, az interneten átívelő alkalmazásoknál nem. A *WS- BusinessActivity* egy olyan keretrendszer és protokollgyűjtemény, amely a lazán csatolt integrált alkalmazások megszakításának koordinálására szolgál.

A megbízható üzenetküldés támogatása a Web szolgáltatások esetében egyszerűen azt jeleni, hogy biztosítjuk azt, hogy minden elküldött üzenet biztosan célba ér pontosan abban a sorrendben, ahogy elindítottuk őket. A *WS-ReliableMessaging* nem garantálja a biztos célba érést egy fellépő meghibásodás esetén, de a ***üzenet kezelős sor*** (message queue) megoldások képesek erre egy állandó, perzisztens tár használatával.

5.7.1 WS-Security

A nyilvános kulcsú infrastruktúra (*PKI*), az *SAML* és a hasonló szabványosítási erőfeszítések és szolgáltatások megvalósítása tudja segíteni a Web szolgáltatásokkal kapcsolatos biztonsági problémák kezelését.

Web szolgáltatás biztonsága WS-Security**WS-Security** (**Web Services Security, röviden WSS**) A SOAP üzenetcsere protokoll kiegészítése, amelynek segítségével a Web szolgáltatások biztonsági sajátosságait lehet definiálni.

- **A WS-* (Web szolgáltatás)** leíró szabványokhoz tartozik (OASIS[8])

Ez a Web szolgáltatás leíró szabvány és protokoll az üzenetek **integritására** (*épségét, sértetlenségét*) és **titkosítására** (*rejtjelezésére, sifrírozására*) vonatkozó szabályok leírását teszi lehetővé, és ezen keresztül határozza meg a tikosítás módját és az integrítás érdekében hozott óvintézkedéseket. Sokféle biztonsági zsetont (tokent) támogat; nevezetesen például : X.509, *SAML*, *Kerberos, PKI*. A fő hangsúly ennél a protokollnál az *XML Signature* és az *XML Encryption* használatán van.

Az *SAML* protokoll a biztonsággal kapcsolatos három lényeges információ kicserélését támogatja a tények megerősítése végett:

(1) a hitelesítést (*authentication*),

(2) a jogosultságok megadását (*authorization*) – mely szolgáltatások használatára jogosult vagy nem jogosult –;

(3) és a szolgáltatás sajátosságaitól függő egyéb attribútumok értékének ellenőrzését és érvényesítését; a szolgáltatásra előírt szervezeti (vállalati, üzleti) szabályok betartása végett

azért, hogy a szolgáltatással végrehajtandó műveletek elvégzésének engedélyezés megtörténhessen.

Ezekre az információcserékre vonatkozó előírásokat *XML* dokumentumok formájában rögzítik. Az *SAML* ezen kívül *kérelem-válasz* (*request-response*) üzenet párok leírását, definiálást teszi lehetővé azért, hogy a ***megerősítésekhez*** (*assertions*) szükséges információcserék lefolytathatók legyenek.

A *WS-Security* az *SAML* protokoll biztonsági ellenőrzéseihez kapcsolódóan azt írja le, hogy ezek a *megerősítések* (assertion) és egyéb biztonsági *zsetonok* (*token*) hogyan kapcsolódnak a SOAP üzenetek fejlécéhez. Ez a SOAP üzenet protokoll sajátosságainak kibővítése, amelynek révén ez a protokoll kiterjesztés *védelmi óvintézkedésekről* gondoskodik, nevezetesen az üzenetek *integritásának* (épségének, sértetlenségének), *bizalmasságának* (confidentialíty) és az adott üzenet *hitelességének*/*hitelesítésének* (authentication) a védelméről. E célok megvalósítása érdekében több biztonsági modellt, mechanizmust lehet alkalmazni: *PKI*, *SSL*, *X.509*, *Kerberos*:

1) X.509 *tanúsítványok (certificate)*;
2) Kerberos „*jegyek*” (tickets);
3) Felhasználó azonosító / jelszó megbízólevél;
4) SAML-*Assertion* (*megerősítés*);
5) Felhasználó által definiált zseton (token).

A *WS-Security* három fő mechanizmust ír le:

- Hogyan azonosítsuk a SOAP üzeneteket, hogyan őrizzük meg az üzenetek integritását. Az üzenetek jelölése "*letagadhatatlan*" (*non-repudiation*) legyen.
- Hogyan titkosítsuk (rejtjelezzük, sifrírozzuk) a SOAP üzeneteket.
- Hogyan csatoljunk az üzenetekhez olyan biztonsági zsetonokat (tokeneket), amellyel meggyőződhetünk a küldő személy azonosságáról.

A specifikáció lehetőséget ad különböző aláírás formátumok, titkosítási algoritmusok és több bizalmi tartományok használatára.

5.7.2 WS-Trust

A *WS-** szabvány család része, amelyet szintén az OASIS[8] dolgozott ki. A WS-Trust egy olyan keretrendszert nyújt, amelynek segítségével egy bizalmi hierarchiát vagy hálózatot lehet ki-

alakítani. Valójában egy olyan Web szolgáltatás, amelyik biztonsági zsetonok (token) kiadásáért, megújításáért és ellenőrzésért felel.

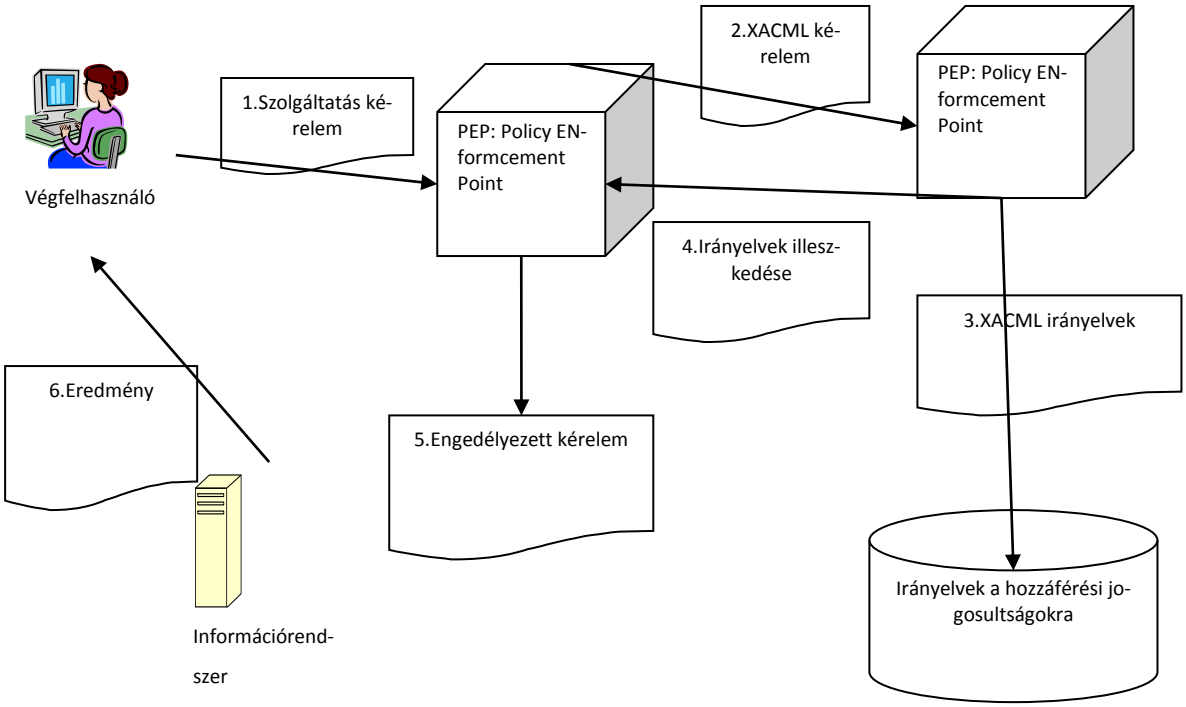
Két fél közötti biztonságos információcsere megvalósítása érdekében a két fél között olyan információcserének kell lefolynia, amelyben felek azonosságnak igazolására szolgáló igazolványok, ***bizonyítványok*** (*credentials*) cseréjére sor kerül. A bizonyítványok cseréje közvetlenül vagy közvetve is történhet (egy megbízható harmadik fél közbe iktatásával), a *WS-Security* protokoll segítségével. Azonban mindegyik résztvevő félnek meg kell bizonyosodnia arról, hogy vajon megbízhatnak-e a másik fél bizonyítványában. A **Web Services Trust** (*WS-Trust*) nyelv a *WS-Security* biztonságos üzenetcsere mechanizmusát használja fel arra célra, hogy további elemi nyelvi egységeket (primitíveket) és további kiegészítéseket definiáljon a biztonsági zsetonok (tokenek) kibocsátásár, cseréjére és érvényességük ellenőrzésére. Ily módon a ***kölcsönös bizalom*** a *biztonsági zsetonok (tokenek) cseréjén, közvetítésén és érvényesítésén keresztül jön létre és reprezentálódik*. *WS-Trust* a különböző bizalmi tartományok között, igazolványok, bizonyítványok kiadására és szétosztására, eljuttatására szintén rendelkezik egy mechanizmussal. Az alkalmazások, Web szolgáltatások felhasználva ezeket a biztonsági mechanizmusokat, biztonságos módón tudnak információt cserélni, miközben természetesen a Web szolgáltatások keretrendszerére támaszkodnak: ***SOAP+WSDL+UDDI+HTTP***.

Egy Web szolgáltatás először a biztonsági sajátosságait a ***WS-Policy*** formájában fogalmazza meg, deklarálja (*claims*). Amikor SOAP üzenet formájában egy olyan **szolgáltatási kérelem** (*request*) érkezik meg egy Web szolgáltatáshoz, amely tartalmaz egy biztonsági zsetont (token), akkor a *WS-Trust* megköveteli, hogy az előírt biztonsági igényeknek feleljen meg, azonosítsa magát a nevével, kriptográfiai kulccsal, és (műveleti) engedélyekkel (*deklaráció*). Egyébként a Web szolgáltatás tudomást sem vesz a kérelemről, vagy megtagadja a kérelem kiszolgálását. A *kérelem* valósiságának és érvényességének ellenőrzése céljából, a Web szolgáltatásnak rendelkeznie kell egy „*bizalmi motorral*” (*trust engine*), szoftver modullal, amely:

1) Leellenőrzi, hogy a kérelmező szolgáltatás deklarációi (*claims*) illeszkednek-e a szolgáltatás által előírt, a biztonsági irányelvekben (*WS-Policy*) szereplő követelményekhez;
2) Leellenőrzi, hogy az elektronikus/digitális aláírás bizonyítja-e, hogy a deklarációt tevő állításai megfelelnek-e a valóságnak;

3) Leellenőrzi, hogy a biztonsági zsetonok (tokenek) megbízhatóak-e abból szempontból, hogy az állításokat, deklarációkat alátámasszák.

Alternatív lehetőség az, hogyha egy megbízható harmadik fél ellenőrzi és igazolja a kérelmező állításait, deklarációit azzal, hogy alátámasztja a kérelmező azonosságát.



14. ábra. XACML használata

5.7.3 XACML

Az **eXtensible Access Control Markup Language** egy OASIS[8] *XML* szabvány specifikáció a hozzáférési jogosultságok és azok ellenőrzésének leírására. *XML*-ben lehet a biztonsági irányelveket megfogalmazni az Interneten keresztül történő információ elérések felügyeletére. Miután elkészítették (megkonfigurálták) ezt a leírást, tartalmazni és publikálni fogja azokat a szabályokat és irányelveket, amelyeket egy hozzáférési jogosultság ellenőrzési mechanizmus meg tud fogalmazni az *objektumok* és azok *attribútumainak* elérhetőségéről. *XACML* két ***architektúra komponenst*** tételez fel: egy biztonsági irányelvek kikényszerítésére szolgáló komponenst, *Policy Enforcement Point (PEP)*, amelyik arról dönthet, hogy vajon egy kérelem kiszolgálható-e vagy sem. Továbbá egy irányelv értékelési komponenst, *Policy Enforcement Point (PEP)*, amely arról hoz döntést, hogy egy irányelv jellegű kérelem engedélyezhető-e. A

PEP egyeztet a *PDP*-vel, a PDP egyeztet az XACML repozitóriumával , adatszótárával. Az ábra (19. ábra)

XACML egyrészt egy **hozzáférési jogok irányelveinek felügyeletét leíró nyelv** (ami lehetővé teszi a fejlesztő számára, hogy deklarálja azt, hogy *ki mit* és *mikor* tehet meg), másrészt a szolgáltatási **kérelmek** és **válaszok** kifejezésére szolgáló nyelv. Ez a nyelv olyan lekérdezések leírására alkalmas, amelyekkel megvizsgálható, hogy vajon egy bizonyos kérelem engedélyezhető-e vagy sem, és a válasz leírását is megadja erre a lekérdezésre. Az XACML specifikációja megadja azokat a definíciókat, amelyeknek segítségével a szabályok lekódolhatók, a szabályokat irányelvekbe lehet összefogni, és azokat az algoritmusokat is meg lehet fogalmazni, amelyeket akkor kell alkalmazni, amikor több szabály is alkalmazható volna. A *hozzáférési ellenőrzési lista* (*ACL, Access Control List*) négy tömbből áll:

1) Az **alany (subject)**: Ez lehet felhasználói azonosító, szerepkör, csoport; pl. „Csak részlegvezetők és magasabb beosztásuk tekinthetik meg ezt a dokumentumot.”
2) **Cél tárgy (target object)**: Ez egy *XML* dokumentum elem, valamilyen hardver/szoftver eszköz, meghajtó, vagy adatállomány lehet.
3) **Tevékenység (Action)**: A megengedett művelet : CRUD, LOAT.
4) **Szabály szolgáltatás (Provision)**: Ez egy olyan tevékenység, amelyet akkor kell végrehajtani, amikor egy XACML szabály aktiválódott; egy ilyen tevékenység lehet riasztás küldése, további igazolások, bizonyítványok bekérése, vagy egy bejelentkezési eljárás megkezdése.

5.7.4 Logikai következtetések levonása a biztonsági irányelvekkel kapcsolatban

Az *XACML* a hozzáférési jogosultságok ellenőrzésére vonatkozó irányelveket reprezentálja, leírja, de nem határozza meg, hogy milyen eljárással történjék meg ez az ellenőrzés. A deklaratív megfogalmazásokat egy ***szabályalapú*** nyelvvel lehet értelmezni, amely kifejezetten a biztonsági irányelvek interpretálását is lehetővé teszi.

Egy ilyen szabályalapú nyelv a következő fogalmakat használhatja:

- **Delegálás** (*Delegation*): Létfontosságú sajátosság a Web szolgáltatások számára, mivel a szolgáltatások nem tudják előre megjósolni, hogy ki intéz kérelmeket hozzájuk, és nem tudják előre azokat a követelményeket sem, amelyeket vele szemben támasztanak a hozzá kérést intéző Web szolgáltatások, entitások. Ha egy entitás megkapja egy bizonyos szolgáltatás elérésére vonatkozó hozzáférési jogokat, ez az entitás to-

vább adhatja, delegálhatja e jogokat megbízható entitások számára anélkül, hogy a a kérelmezett szolgáltatás biztonsági irányelveit és követelményeit explicit módon meg kellene változtatni.

- **Visszavonás (***revocation***):** Egy olyan információtovábbítási lépés, amely egy entitás létező jogosultságait lenullázza, akár irányelvek révén jutott hozzá, akár delegálás útján.
- **Kérelem (***Request***)**: egy másik entitáshoz intéz kérelmet, hogy megkaphasson egy jogosultságot vagy végrehajthasson egy *cselekményt* (*action*).
- **Törlés (***Cancel***)**: Egy korábbi kérelem visszavonása.

Irányelvek közti konfliktusok nyílt rendszerekben teljesen természetesek. Ezért egy szabályalapú rendszernek tartalmaznia kell, konfliktus feloldó mechanizmusokat:

1) Modalitási rangsor, preferencia beállítás (negatív a pozitívval szemben, vagy fordítva);
2) Az irányelvek közötti rangsor, preferencia felállítása.

A hozzáférési jogosultságok jelenlegi kezelési mechanizmusának egy hibája az, hogy együttesen kezelik a hitelesítés, jogosultság megadás, és hozzáférési jogok ellenőrzését (authentication, authorization, access control). Ha egy adatfeldolgozási folyamat egy végfelhasználó azonosítása alapján megkap bizonyos jogokat, akkor az összes további adatfeldolgozási folyamat, amely a felhasználó nevében jár el, megkapja ugyanazokat a jogosultságokat és privilégiumokat. Ha az adatfeldolgozási folyamatot ellenséges támadás éri, pl. vírus fertőzés, akkor a felhasználó teljes számítógép környezete veszélybe kerül; adatállományok, elektronikus levelek, adatbázisok, hálózati kapcsolatok.

Ennek a problémának kezelésére a legkisebb felhatalmazás elvét vezették be (principle of least authority (POLA)). Az adatfeldolgozási folyamatoknak és objektumoknak csak annyi jogosultságot és felhatalmazást adnak meg, amennyi ahhoz szükséges, hogy elvégezzék feladataikat és elérjék céljaikat. Ezen kívül a jogosultság kibocsátás három aspektusának (hitelesítés, jogosultság megadás, és hozzáférési jogok ellenőrzése (authentication, authorization, access control)) kezelésének szétválasztása is szükséges azért, hogy egy finomabb felbontású engedély és jogosultság felügyeletet lehessen megvalósítani.

5.8 Egyszeri bejelentkezés és föderatív személy azonosítási protokoll

Security Assertion Markup Language (**SAML**) az informatikai iparon belül domináns pozícióban lévő protokoll és nyelv a **föderatív személy** (és egyéb) **azonosítás** területén, a telepített

és üzemelő rendszerek tekintetében. Elsősorban a mai számítási felhőnek nevezett, Interneten keresztül nyújtott szolgáltatásokkal kapcsolatban több tízezer rendszert helyeztek üzembe; elsősorban nagyvállalatok, kormányzati szervezetek és egyéb Interneten keresztül szolgáltatást nyújtó cégek számára.

5.8.1 Alapműködési modell

2002-ben bocsátották ki *SAML* az 1.0 verziót, amely éveken keresztül fejlődött, 2005-ben jelent meg a SAML 2.0 verzió. SAML szabvány gazdaszervezete **OASIS** Security Services Technical Committee.

SAML 2.0 három föderatív azonosítási szabvány kombinációja: SAML 1.1, ID-FF (Identity Federation Framework) 1.2, és Shibboleth.

5.8.2 Előnyei

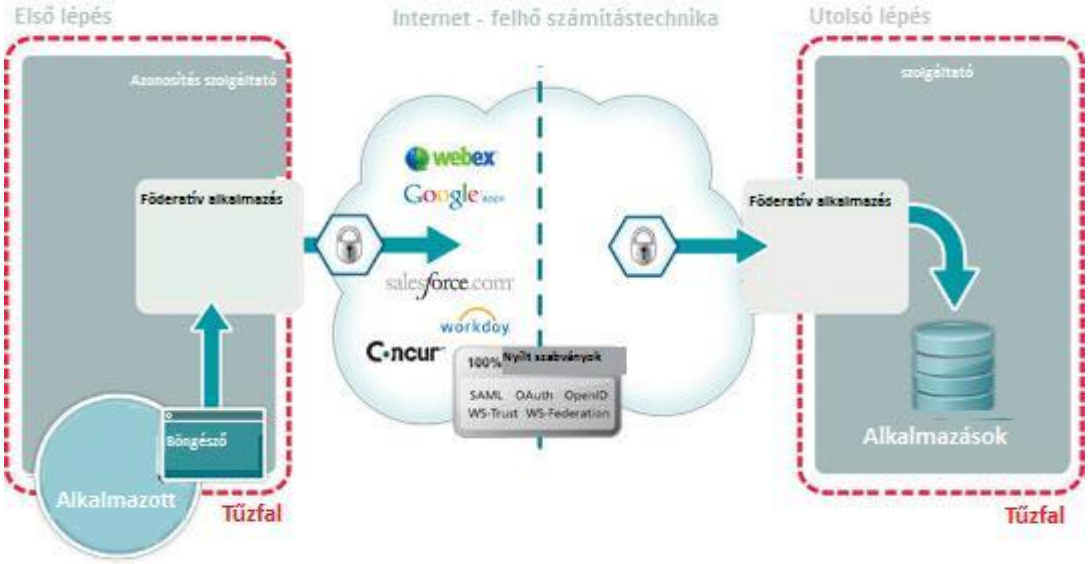
SAML XML alapú, ezért rugalmas, könnyen kiterjeszthető, bővíthető szabvány. A föderációba tartozó két tetszőleges partner kiválaszthatja azt, hogy melyik azonosítást lehetővé tevő attribútumot akarják felhasználni közösen. A SAML üzenetek tartalmában ezt tudják használni, feltéve, hogy a kiválasztott attribútum ábrázolható XML-ben. Ez a rugalmasság természetesen SAML rész szabványokhoz vezet, mint pl. az SAML azonosítás **megerősítés** (**assertion**), illetve a *SzOA* architektúrához tartozó **WS-Federation** szabványokba történő beillesztése.

Az SAML különös előnye az együttműködési, interoperabilitási képesség több olyan gyártói SSO megoldással szemben, amelyek megkövetelik, hogy mind a szolgáltató (*Service Provider-t (SP)*) mind az azonosítás szolgáltató (*Identity Provider-t (IdP)* ugyanazt a szoftvert, rendszert telepítse és helyezze üzembe. Ez egy nagyvállalat vagy közigazgatási szervezet számára azt jelenti, hogy minden egyes új kapcsolatrendszer egy új és esetleg egy teljesen különböző szoftver telepítését igényli. Ezzel szemben az SAML egy üzembe helyezett példánya támogatni tudja az SSO kapcsolatokat több, különböző föderatív partnerrel.

Ezért az SAML különösen alkalmas felhő-számítástechnika (*Cloud Computing*), alkalmazás szolgáltató (ASP) vagy bármilyen más külső, Interneten keresztüli szolgáltatókkal kapcsolatban az egyszeri bejelentkezés megvalósítására (SSO) akkor, amikor a szolgáltatás igénybevétele a ***szoftver mint szolgáltatás*** minta alapján valósul meg (*Software-as-a-Service (SaaS)*).

5.8.3 SSO az Interneten keresztül és föderatív azonosítás

A föderatív azonosítás azt jelenti, hogy felhasználói, személy azonosságok biztonságosan megoszthatók legyenek eltérő hálózati tartományok és alkalmazások között. Az SAML és a WS-Federation az a két alapvető szabvány és ezek változatai, amelyeket a gyakorlatban használnak (SAML 1.0, SAML 1.1 and SAML 2.0.).



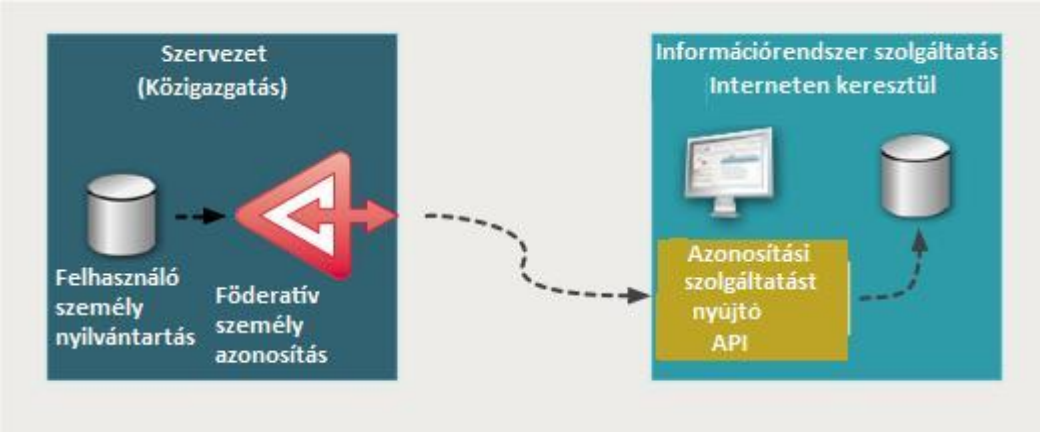
15. ábra Föderatív azonosítás és egyszeri bejelentkezés alap architektúrája

5.8.4 Modellek: Internet szolgáltatások használata egyszeri bejelentkezéssel

Három modell különböztethető meg.

5.8.4.1 1. szint: SSO (egyszeri bejelentkezés): Interneten keresztül nyújtott szolgáltatások használatára stratégia

Ez a stratégia szabvány-alapú internet tartományokon keresztül nyúló azonosítás megoldásáról gondoskodik.



16. ábra A szervezetnél nyilvántartott azonosságokban bekövetkezett változásokat megduplikálja a szolgáltatónál létező nyilvántartásokban.

Az 1. szint bevált szabványokon alapul, amely web alapú párbeszédes kapcsolatokat köt össze alkalmazásokkal és egy központi nyilvántartásban hajtja végre az azonosság hitelesítését, amely a szabályok betartásának, betartatásának és felügyeletének egyetlen ellenőrzési és referencia pontja. Az 1. szintű SSO esetében sem jelszavak küldésére nem kerül sor, sem a felhasználó bejegyzések megduplikálására – a felhasználói azonosságok fölött felügyeletet az azonosítót kibocsátó szervezet informatikai részlege látja el.

Előnyei:

1. Maximális biztonság Interneten keresztüli szolgáltatások igénybevételekor.
2. A legkényelmesebb megoldás az összes érintett félnek: felhasználók, informatikai részleg/ funkció és alkalmazás szolgáltatók.
3. Felhasználói jelszavakat egyszer tárolják el, egy olyan helyen, amelyet szervezet megfelelően tud védeni.
4. A legmagasabb megbízhatóságot nyújtja miközben a böngészők és az alkalmazások folyamatos frissítéseken esnek át.
5. Nincs gyártó függőség a szabványoknak köszönhetően.
6. Általában a legalacsonyabb a teljes bekerülési és üzemeltetési költség (total costs of ownership, TCO).

Hátrányok

1. A modell egyes konkrét megvalósításaiban, az azonosítással kapcsolatos szakértelemnek közvetlenül rendelkezésre kell állnia.

2. A föderációban részt vevő feleknek a megvalósítás érdekében együtt kell működniük.

Az 1. szintű SSO meghatározó jellegzetessége az, hogy az azonosítást és hitelesítést szabványon alapuló zseton, 'token' cserével oldja meg, a felhasználói nyilvántartások azonban központilag kezelt tartományon belül maradnak és nem szinkronizálják más külső erőforrásokkal. Az alkalmazásokba történő bejelentkezésnél a jelszó használatot felszámolják, jelszóra nem lesz szükség kivéve a felhasználói nyilvántartásokra támaszkodó azonosítási és hitelesítési folyamatokat, mint pl. a Microsoft LDAP-ja, az Active Directory-ból (MS AD) történő azonosítás és hitelesítései eljárás lefolytatásához. Minden azonosítással kapcsolatos információ kriptográfiailag védetten közlekedik a hálózaton. Az 1. szintű SSO a nyílt és bevált szabványokon alapszik, nevezetesen az SAML, az OpenID Connect[9]-en és az OAuth[10].

1. szintű SSO megoldásnál, amikor egy kapcsolatot felépítenek egy alkalmazással, a SSO szolgáltatás kikerül az információcsere folyamatából miután a párbeszéd már létrejött az érintett rendszerek között, más modelleknél az információcsere közepén marad egy állandó **proxyként** (**közvetítő ügynök**), amelyen keresztül kell az információáramlásnak megtörténnie. 1. szintű SSO megoldást a következő célok indokolják: az ügynök maximalizálja (1) az információcsere áteresztőképességét, (2) csökkentse a késleltetést, (3) számolja fel az egypontos *hibagócot* (single point of failure), és (4) küszöbölje ki a személyes adatok és magántitkok esetleges megsértésének veszélyét.

Vannak olyan indokolt esetek, amelyekben a *proxyra* szükség van, különös egyes ipari ágazatokban, gazdasági szektorokban, azonban ez a proxy/ügynök modell inkább kiegészítő szolgáltatásnak tekinthető semmint a 1. szintű SSO modell lényegéhez tartozó megoldásnak.

5.8.4.2 2. szintű SSO: Saját, egyetlen hálózati tartományra vonatkozó azonosítás

A **2. szintű SSO** olyan szervezetekben szükséges, ahol sok régi és elavult, korszerűtlen alkalmazás található, és amelyek nem integrálhatók be a modern felhasználói nyilvántartásokba, mint pl. a Microsoft AD-be. A 2. szintű SSO modellt megvalósító gyártói implementációk alkalmazkodtak a felhő-számítástechnika, vagy általánosabban az Interneten igénybe vett szoftver szolgáltatásokhoz, a Web Access Management[11] megközelítés révén. A *2. szintű SSO* modell a szoftver mint szolgáltatás jellegű alkalmazások (SaaS) számára tulajdonképpen egy szub-optimális megoldás, amely lehetővé teszi az olyan régi és elavult alkalmazások életcik-

lusának kiterjesztését, amelyek nem tudnak váltani a régi *azonosítási*, *hitelesítési* és *jogosultság kezelési* módszereikről az újra.

Előnyök

1. Az olyan régi elavult alkalmazási rendszerekben is megszabadulhatnak a jelszó használatától, amelyekben a modern felhasználói nyilvántartások nem használhatók.
2. Központosított, hálózati tartomány központú, információcserét nyújt, amelyben keretében a biztonsági irányelvek betarthatók.
3. A 2. szintű SSO modellhez szükséges komponensek esetleg már rendelkezésre állnak, és az SSO megvalósításához szükséges kezdeti lépésekhez elegendő funkcionalitást tudnak nyújtani.

Hátrányok

1. Általában gyártó, vagy tulajdonos függő, jelentősen módosították a testre szabhatóság végett.
2. Magas bekerülési és üzemeltetési költségek.
3. Mind a böngészők mind az alkalmazások kézben tartása szükséges, vagy a rendszer összedől.
4. A felhő-számítástechnikához, vagy általánosabban az Interneten keresztül igénybe vett szoftver szolgáltatásokhoz. nem igazán illeszkedik.
5. A biztonsági sebezhetőség lehetősége több ponton is fennáll.

A *2. szintű SSO* modell valójában érett technológia, van vonzereje, azonban egyedi, gyártói technológiát használ általában a felhasználó által kezdeményezett ember-gép párbeszéd nyomon követésére. Web Access Management esetében kriptográfiailag védett sütiket használnak az állapot megőrzésre – azonban ez a megoldás a felhő-számítástechnika esetében nem működik a sütik másféle kezelése miatt. 2. szintű SSO modell zseton, token alapú protokolljai (pl. ***Kerberos***) pedig nem tudnak több hálózati tartományon keresztül működni. Néhány 2. szintű SSO modell ezt úgy próbálja áthidalni, hogy 1. szintű SSO modell egyes funkcionális szolgáltatásaira próbál támaszkodni, ezek lehetnek például az SAML modulok. Más 2. szintű SSO modell megvalósítások pedig a 3. szintű SSO modell olyan funkcionalitását kívánják felhasználni, mint például a képernyő tartalom lelopása vagy a jelszavak megduplikálása.

5.8.4.3 3. szintű SSO modell: azonosítók visszajátszása, tartományokon keresztüli azonosítás és hitelesítés

3. szintű SSO modellben a felhasználói neveket és jelszavakat az adott szervezet informatikai funkciójának, részlegének hatás körén kívül tárolják, és a szóban forgó alkalmazások számára a felhasználói neveket és jelszavakat az Interneten keresztül visszajátsszák az adott alkalmazásnak. Ez a megoldás gyors probléma kiküszöbölés, amely megszabadít a felhasználói jelszavak kezelésétől, és újra beállításától, de ennek az ára a biztonságirányítási szabályozás és irányelvek optimális megvalósíthatóságának elvesztése. Egyes iparágakban és gazdasági szektorokban nem felel meg a szabályozó hatóságok előírásainak.

Előnyök:

1. Viszonylag alacsony bevezetési költségek (az eszközök általában ingyenesek).
2. A felhasználók a személyes adataikat egy tároló helyen tudják tartani valahol az Interneten.

H**átrányok:**

1. Magas biztonsági kockázatok - a legtöbb megoldásnál a felhasználó tudja meghatározni a jelszó kriptográfiai erősségét; nem-SSL Internet tartományok esetében az azonosításra szolgáló adatok kriptográfiai védelem nélkül közlekednek az Interneten.
2. Folyamatos napra készen tartást igényel, mivel a jelszó átadás mechanizmusa elakad minden olyan estben , amikor az alkalmazás, web hely tulajdonos, internet szolgáltatója megváltoztatja bejelentkezési mechanizmust illetve képernyőt.

3. szintű SSO modellben több architekturális megoldás között lehet választani. Lehet a felhasználói nyilvántartás adatbázisát valahol az Interneten, a felhőben tartani, vagy magánfelhőben, helyi kiszolgálón vagy akár egy alkalmazott asztali számítógépén. 3. szintű SSO modell főbb jellemzői:

1. Legalábbis részlegesen egy egyedi adattárhelyre kell támaszkodni a felhasználói nevek és jelszavak tárolásánál szemben a zseton, token alapuló információcserével.
2. A személynek saját magának kell gondoskodnia az azonosító adatok bejuttatásáról az adatbázisba. Néhány 3. szintű SSO modell automatikusan felerősíti a jelszót és a felhasználó elöl el is fedi.

3. Ez a megoldás támaszkodhat egy központi felhasználó nyilvántartásra, amelyet azonban elsődlegesen arra használnak, hogy feltöltsék az adatbázist.
4. 3. szintű SSO modell részben olyan szolgáltatók azonosítási szolgáltatásaira támaszkodnak mint például a „Facebook" vagy az „MSN Live".

Ez a 3. szintű SSO modell fokozza a felhasználók kényelem érzetét és csökkenti az informatikai részleg adminisztrációs terheit (kevesebb jelszó beállítás). Azonban ebben a modellben nehéz egy központi személy azonosítási *irányelvet* és *szabályzatot* érvényesíteni. A konkrét megvalósítások általában lehetővé teszik, hogy felhasználó saját maga által előállított felhasználó nevet és jelszót használjon.

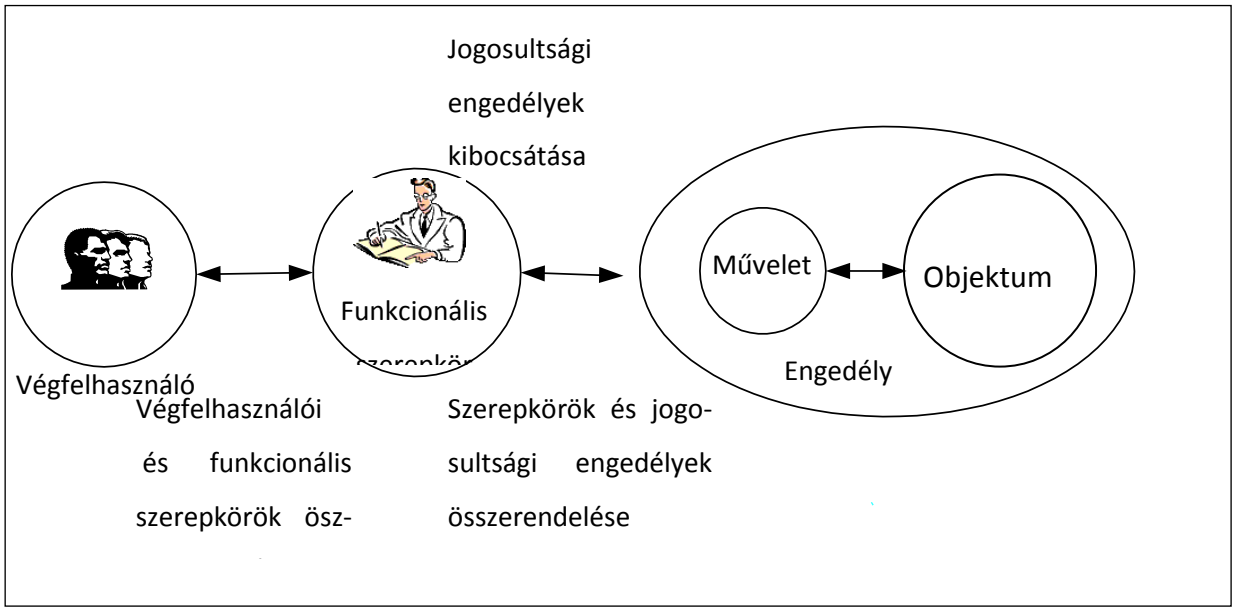
5.9 Jogosultsági viszonyok ábrázolására szolgáló architektúra megoldások

A ***hozzáférési jogosultságok leírása*** alapvetően két bevált módszer áll rendelkezésre a **szerepkör alapú** és az **attribútum** (sajátosság, tulajdonság) **alapú jogosultsági rendszer**. E két rendszer kombinálható is.

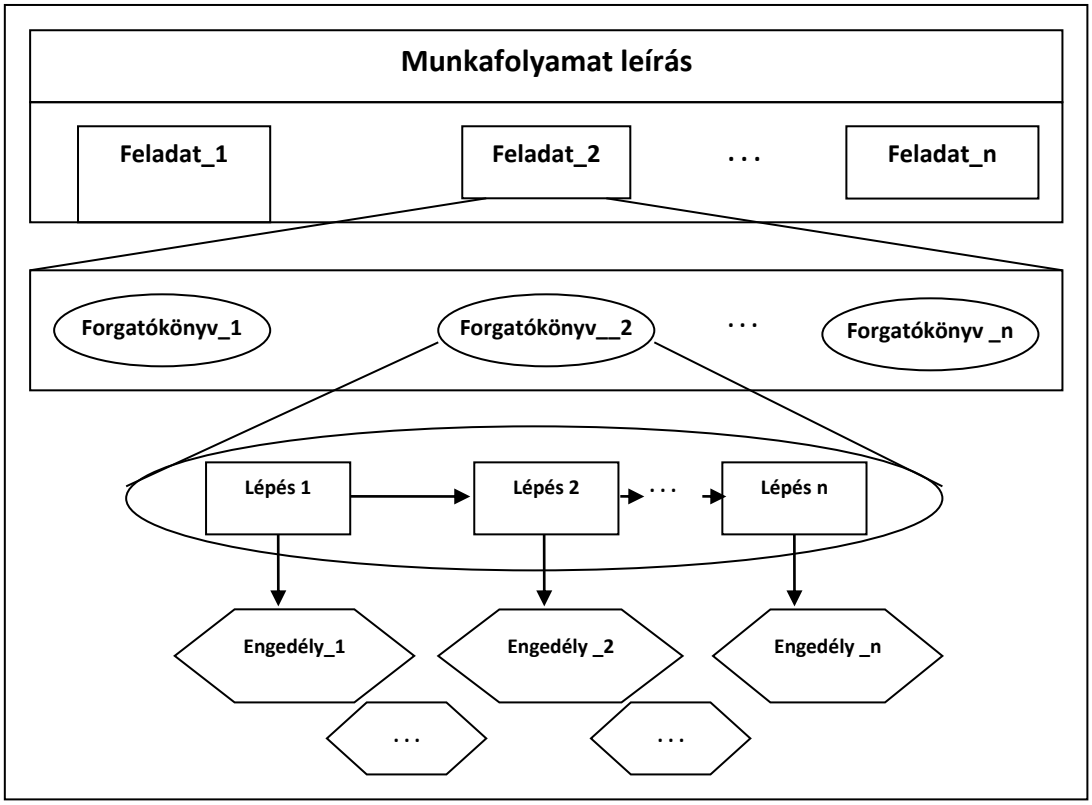
Az információrendszerek alapvető *szereplői* („*actor*") az ügyfél (természetes személy), végfelhasználó, ügyintéző, egyéb belső és külső érintett/érdekelt felek. Illetve az Internet, Web, világháló, számítási felhő kontextusában megjelenik a ***kibertérben létező szervezet*ek** elektronikus megszemélyesítése, mint potenciális szereplő, aki számára jogosultságokat kell kibocsátani (pl. virtuális vállalkozások, „Virtual Enterprises").

Az egyik jogosultsági dimenzió az elektronikus/informatikai hozzáférési jogosultság. A másik az ügyintézés, ügyvitel, üzletvitel viszonylatában a szervezeti (vállalati, üzleti) folyamattal kapcsolatos, feladatkör, hatáskör, felelősségi kör, rendelkezési jog, felhatalmazott, meghatalmazott, saját jogon, önállóan jár el stb.

A rendszerrel érintkezésbe lépő szereplők (ügyfél, meghatalmazott, megbízott, ügyintéző, végfelhasználó stb.), amikor a *kibertérbe* kerülnek és ott tevékenykednek akkor a feladataiknak, jogosultságaiknak leképezése a kibertérben használható fogalmakra a *hozzáférési és adatkezelési jogosultsági rendszeren* keresztül ragadható meg. E hozzáférés *jogosultsági* rendszer a kibertér alapfogalmaival dolgozik: adat, e-dokumentum vagy objektum, amelyeken *műveletek* bizonyos elektronikus adatfeldolgozó tevékenységek elindítása révén hajthatók végre.



17. ábra A jogosultságok megadásának alapsémája egy elektronikus információrendszer környezetben



18. ábra A jogosultsági engedélyek és forgatókönyvek lépéseinek összekapcsolása munkafolyamat munkafeladatain belül

6 BIBLIOGRÁFIA

1. Ali Arsanjani, Toward a pattern language for Service-Oriented Architecture and Integration, Part 1: Build a service eco-system, http://www.ibm.com/developerworks/webservices/library/ws-soa-soi/index.html , 2011-08-21
2. Bieberstein-Bose-Fiammante-Jones-Shah, *Szolgáltatás-orientált architektúra*, PANEM, Budapest, 2009.
3. Breuer H. [1995]: Informatika, SH Atlasz, Springer-Verlag Budapest, Berlin
4. Brooks, F. *The Mythical Man-Month: Essays on Software Engineering.* Addison-Wesley, 1975.
5. Bundesamt für Sicherheit in der Informationstechnik(BSI): *Eckpunktepapier. Sicherheitsempfehlungen für Cloud-Computing-Anbieter*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf;jsessionid=07F82607FB8632F14F0DC0A96F9BD4F9.2_cid286?__blob=publicationFile (letöltve: 2012.10.30.)
6. D. Garlan, M. Shaw, An Introduction to Software Architecture, Advances in Software Engineering and Knowledge Engineering, Volume I, World Scientific, 1993.
7. Daniel Minoli, Enterprise Architecture A to Z Frameworks, Business Process Modeling, SOA, and Infrastructure Technology, Auerbach Publications, Taylor & Francis Group, ISBN 978-0-8493-8517-9, 2008
8. Daniel Minoli, Enterprise Architecture A to Z Frameworks, Business Process Modeling, SOA, and Infrastructure Technology, Auerbach Publications, Taylor & Francis Group, ISBN 978-0-8493-8517-9, 2008
9. Davenport, T. H. – Short, J. E. (1990): The New Industrial Engineering: Information Technology and Business Process Redesign, in Sloan Management Review, 1990. Summer
10. Davenport. T. H. (1993): Process Innovation: Reengineering Work Through Information Technology, Harvard Business School Press, Cambridge, MA
11. D-Grid-Projekts FinGrid (2009): Grid Computing in der Finanzindustrie. Publication 01/2009, *efinancelab* Frankfurt/M, Books on Demand GmbH, Nordenstadt.

12. Dirk Matthes, Enterprise Architecture Frameworks Kompendium, © Springer-Verlag Berlin Heidelberg 2011, e-ISBN 978-3-642-12955-1, ISSN 1439-5428
13. Emilia Mendes · Nile Mosley (Eds.), Web Engineering, Springer-Verlag Berlin Heidelberg, 2006,
14. Eric Newcomer, Greg Lomow, Understanding SOA with Web Service, Addison Wesley Profession, 2004, ISBN: 0-321-18086-0
15. Erl, Thomas, Service-Oriented Architecture Concepts, Technology and Design, 2005, Pearson Education
16. Fröschle, H-P. (Fröschle, 2011): Cloud Computing - Herausforderungen für IT-Management und –Betrieb. *ERP Management*, Nr. 1/2011, S. 45-46
17. Holtz, P. Cloud biztonság, http://www.bitport.hu/biztonsag/cloud-biztonsag-szakertoi-cikk-holtzl-peter (letöltve: 2012.08.07.)
18. Jack Wout, et al. *The integrated architecture framework explained : why, what, how.* Springer, 2010. ISBN 978-3-642-11517-2, DOI 10.1007/978-3-642-11518-9
19. Jeffrey Zeldman, Designing With Web Standards, New Riders Publishing, 2003, ISBN, 0-7357-1201-8
20. Jim Conallen, Building Web Applications with UML, Second Edition, Addison Wesley, 2002, ISBN, 0-201-73038-3
21. John A. Zachman (2009): The Zachman Framework: The Official Concise Definition http://test.zachmaninternational.com/index.php/the-zachman-framework , 2011-08-18
22. Kaisha Tec (2009): BPMN - Business Process Modeling Notation 1.2 Poster, http://www.active-flow.com/download/Documents/Poster_BPMN.pdf Letöltve: 2010. március 16.
23. Lankhorst,M., et al. (eds.): *Enterprise Architecture at Work: Modelling, Communication and Analysis*. Springer, Berlin (2005), ISBN-10: 3540243712
24. Li, Qing – Chen, Yu-Liu (2009): Modeling and Analysis of Enterprise and Information Systems – From Requirements to Realization, Springer Berlin Heidelberg
25. M. Havey *Essential Business Process Modeling*, O'Reilly , 2005, ISBN: 0-596-00843-0
26. Marc Lankhorst et al., Enterprise Architecture at Work, 2005, Springer-Verlag Berlin Heidelberg, ISBN-10 3-540-24371-2

27. Martin Op 't Land, Erik Proper, Maarten Waage, Jeroen Cloo, Claudia Steghuis, Enterprise Architecture, Creating Value by Informed Governance, Springer-Verlag Berlin Heidelberg, ISBN 978-3-540-85231-5, 2009
28. Mathias Weske, *Business Process Management, Concepts, Languages, Architectures*, © Springer-Verlag Berlin Heidelberg 2007, ISBN 978-3-540-73521-2 ,
29. Molnár B., [1997]: *Bevezetés a rendszerelemzésbe*, in: Gábor András (szerk.) „Információmenedzsment", Aula Kiadó, 1997, pp 107-239.
30. Molnár Bálint, 'Ismeretszerzés', in: Futó Iván (szerk.) „ Mesterséges Intelligencia", Aula Kiadó, 1999, pp 665-708. http://www.mtaita.hu/KADSbev9_1.PDF , http://www.mtaita.hu/CommonKADS.PDF
31. Molnár Bálint, *Rendszerelemzés,* in: Gábor András (szerk.) „*Információmenedzsment*", Aula Kiadó, CD-melléklet, 1996–98, http://www.mtaita.hu/hu/Publikaciok/Ssadm1.pdf (2011-08-29)
32. Mosley, Mark, et al. DAMA guide to the data management body of knowledge (DAMA-DMBOK guide). Technics Publications, 2010.
33. Oellermann, William L. Jr., Architecting Web Services, Apress , 2001, ISBN:1893115585
34. Open Group, TOGAF: The Open Group Architecture Framework, TOGAF® Version 9, http://www.opengroup.org/togaf , 2010.
35. *Racskó P.* (2012): A számítástechnikai felhő az Európai Unió egén. *Vezetéstudomány*, Nr. 1/2012, 2-16. oldal, ISSN: 0133-0179. Budapest, 2012
36. Repschläger, J., Zarnekow, R.: *IT-Outsourcing und Cloud-Sourcing – Gemeinsamkeiten und Unterschiede.* ERP Management 7 (2011) 1, 48-51. old.
37. The Open Group: *Building return on investment from cloud computing. A white paper, cloud business artifacts project*. Cloud Computing Work Group (2010).
38. TOGAF— *TOGAF Version 9, The Open Group Architectural Framework*, The Open Group, 2009, http://www.togaf.org
39. Voas, J.; Zhang, J.: *Számítási felhő: New Wine or Just a New Bottle?* Computer org/IT PRO March/April 2009. ©Published by IEEE.
40. von der Dovenmühle. T.-, Gómez, J. M. (Dovenmühle et al, 2011): Datenschutz beim Einsatz von Cloud Computing, *ERP Management*, Nr. 3/2011, S. 58-60

41. Was kostet die Cloud? www.login2work.de (letöltve: 2012. 03. 28.)
42. Weinman, J. (2012). *Cloudonomics: The Business Value of Cloud Computing*. Wiley. com.
43. Woojong Suh (ed.): Web Engineering: Principles and Techniques, ISBN 978-1591404330, IGI Global, 2005.
44. Zachman, J.: A framework for information systems architecture. IBM Syst. J. 26(3) (1987)

---

[1] http://ec.europa.eu/news/science/130212_hu.htm

[2] http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf

[3] http://www.kipling.org.uk/poems_serving.htm . „Hat derék szolgát tartok. Ők tanítottak meg engem mindenre, amit csak tudok."

[4] http://zachmanframeworkassociates.com/Standards/protected/framework-graphic-3. 2011-08-18

[5] A kulcsok generálása, létrehozása magasabb biztonsági szint érdekében csak megfelelően elkülönített szoftver és hardver eszközben történhet. Ugyanis a jelenlegi elterjedt operációs rendszerekből a veremben („stack"= operációs adathalma) keletkező kriptográfiai kulcsokat automatikusan továbbítják az Interneten keresztül: ez mind UNIX/LINUX mind a Windows változatokra igaz a patrióta törvény következtében.

[6] http://hu.wikipedia.org/wiki/Elektronikus_al%C3%A1%C3%ADr%C3%A1s

[7] Az EU tagállamokban az a megoldás terjed, hogy a minősített aláírás létrehozására alkalmas tanúsítványt olyan eszközre, adathordozóra helyezik, amelyiknek a biztonsági besorolása egy kicsit gyengébb, ezért a tanúsítvány és az adathordozó eszköz (intelligens kártya, USB) együttese csak fokozott biztonságúnak tekintendő, de ennek jogérvényességét kiegészítő szabályozással biztosítják.

[8] OASIS (Organization for the Advancement of Structured Information Standards): https://www.oasis-open.org/

[9] http://openid.net/connect/

[10] http://oauth.net/

[11] http://en.wikipedia.org/wiki/Web_Access_Management