Vékás Sándor
ügyvezető, IT biztonsági auditor
Közinformatika Közigazgatási Informatikai
Szolgáltató Központ Nonprofit Kft.

Az önkormányzati informatika aktuális feladatai és problémái – információbiztonság, ASP, elektronikus közszolgáltatások, Smart City

A világ lázban ég. A technológiai forradalom új szakaszában az információs forradalom hajnalán járunk. A közigazgatással szembeni elvárások semmivel nem kisebbek, mint az élet más területein tapasztalható várakozások. Az emberek okos városban szeretnének élni, ügyeiket az interneten keresztül szeretnék intézni. Az állam szeretne mihamarabb, minél pontosabb képet kapni az önkormányzatok helyzetéről. Az önkormányzatok pontosan szeretnék ismerni részlegeik, cégeik, vagy akár projektjeik pillanatnyi állapotát. A képviselők szeretnék elektronikusan megkapni az ülések anyagait, a döntéstámogatáshoz szükséges dokumentumokat. Mindehhez informatikai fejlesztések, megoldások, infrastruktúra és azt értő, üzemeltető személyzet szükséges. Az elvárások nagyok, a rendelkezésre álló erőforrások meg szűkösek. Mégis haladnunk kell a korral, mégis meg kell felelnünk a lakosság és az ellenőrző szervek méltányolható elvárásainak. Lemaradásban vagyunk. Se pénz, se szaktudás. Hogyan tudjuk **így** lefaragni a hátrányt? Erre próbálunk választ adni.

Honnan jöttünk?

Az önkormányzati informatika, amióta csak létezik, sosem volt túlfinanszírozott – inkább alul. Kezdetben lelkes amatőrök által összerakott gépeken futó, *„valahonnan akasztott”* operációs rendszereken, helyben írt nyilvántartó szoftverek uralták a területet. Aztán megjelentek a felügyeleti szervek által diktált adatigényelések és az ezeket kiszolgáló fél profi, majd profi szoftvermegoldások. Közben a géppark bővült és fejlődött is, a jogtiszta szoftverek köre is szélesedett, de a mai napig nem lehet kijelenteni, hogy a szektor utolérte volna **ön**magát.

Hová tartunk?

Néha fel-felbukkan egy-egy állami projekt, ami segíteni látszik bizonyos részterületeken, de egységes megoldás ez idáig nem látszott. Most több fronton is változás várható. Egyrészt az ASP pilot fázis nehézségeinek kiküszöbölése után jön végre az új *önkormányzati ASP program,* amelynek célja a sokféle önkormányzati szakrendszer egységesítése, másrészt indulnak a *SZEÜSZ*-ök, azaz a szabályozott elektronikus ügyintézési szolgáltatások, amelyek pedig a lakossági szolgáltatások internetes elérésének lehetőségét tűzték ki célul. Azaz a mindennapi önkormányzati feladatellátás mellett az állammal való kapcsolattartás és a lakossági ügyintézés is sokkal modernebb keretek közé emelkedik. Mindehhez mindenekelőtt persze szélessávú és nagyon stabil internetkapcsolat szükséges, de most ezen a téren is komoly tervek, és ami szintén fontos: komoly EU-s és állami források jelentek meg. Az úton tehát elvileg el tudunk indulni.

Gyökeres változások, új kihívások

De, hogyan kezdjünk hozzá, mi a teendőnk? Várjuk a szélessávot, várjuk az ASP-t és a SZEÜSZ-öket? Ha belátjuk, hogy az eddigiektől egészen sokban különböző, informatikavezérelt világ jön – vagy inkább száguld – felénk, azt is be kell látnunk, hogy az eddig akár elhanyagolt, megtűrt területtel immár nem csak tűzoltásként, hanem egyenesen stratégiailag is foglalkoznunk kell: pénzt és időt is kell rá áldoznunk. Nyilvánvalóan stabilizálnunk kell tehát az informatikát, mind eszköz, mind üzemeltetői, mind felhasználói szinten. Nem működhet egyetlen község sem úgy, hogy nincs legalább egy szerződött szakembere, aki hetente legalább néhány órát ne

töltene el az elektronikus információs rendszerek felügyeletével, karbantartásával. 30-40 munkaállomás fölött pedig nagyon komolyan el kell gondolkodni főállású rendszergazda alkalmazásán. Nem használhatunk tovább mindenhonnan leselejtezett eszközöket, a gyártó által már nem támogatott, nem frissített, operációs rendszereket, amelyek ráadásul nem is feltétlenül jogtiszták. Több éves, festékfaló nyomtatóink és elégtelen védelmet nyújtó ezeréves tűzfalaink szintén nem felelnek meg sem a gazdasági, sem a biztonsági elvárásoknak. A hivatal belső informatikai hálózata, ha van egyáltalán, és a szerverpark, ha van egyáltalán, szintén átvizsgálandó, mert immár nem csak a produktív hivatalon belüli munkavégzés a tét, hanem a várható fejlesztésekhez való biztonságos csatlakozás és működés is.

Az informatikai kultúra

Az eszközparknál és az infrastruktúránál azonban van még nehezebben fejleszthető dolog: az informatikai kultúra. Gyakran megfordulunk olyan hivatalokban, ahol a munkatársak a saját asztali gépük winchesterére mentik a munkájuk során létrehozott, módosított dokumentumokat. Itt a közös munkát legfeljebb az egyik kolleganő asztali gépének megosztott mappája jelenti, hiszen szerver nincsen, de még egy kis *NAS* sem. Olyan helyeken is jártunk, ahol a jelszavak, ha egyáltalán vannak, a monitor sarkára vannak évek óta tűzve, hogy bárki használhassa őket. Van ahol minden dolgozó adminisztrátor a saját gépén, így aztán azt telepít magának, amit csak akar, függetlenül attól, hogy jogtiszta-e, esetleg vírusos-e az adott alkalmazás vagy nem. Persze ahol szerver nincs, ott szerverszoba, vagy rack-szekrény sincs és általában a mentés sem megoldott. De mitől is lenne? Eddig nem kellett, s mivel rendszergazda is csak esetenként, lassítva megy át a falun, senki nem is erőltette ezeket, a munkatársak pedig szintén nem igényelték.

Mindez nem maradhat így, ezt lassan mindenki látja. Jönnek a változások, mi meg itt állunk kevés pénzzel, ismeretek nélkül. Hogyan tudunk felkészülni a változásra? Hol kaphatunk sorvezetőt, mi legyen a stratégiánk? Honnan lesz rá pénzük? Mielőtt ezekre válaszolok, tekintsük át az alábbi szempontokat, váltsunk picit más látószögre!

Terítéken az információbiztonság

A híradások mindennapi, visszatérő témái az információs rendszerek, kormányzati szerverek, portálok elleni támadások. Ilyen támadás érte a közelmúltban Japánt, az USA-t, Észak-Koreát, de sajnos Magyarország kormányzati, sőt önkormányzati oldalait is. Komoly tartalommal, funkcióval bíró kormányzati és multinacionális vállalati rendszerek álltak az elmúlt hónapokban *DDoS*, azaz túlterheléses támadás alatt, amelynek következtében egy ideig elérhetetlenné váltak. A *WikiLeaks, Julian Assange* **és** *Edward Snowden* tevékenysége, vagy az Apple *iCloud*-ból ellopott celeb fotók ügye az átlagember szintjén is legalább csodálkozást, ha nem egyenesen aggodalmat váltott ki. A szomszéd önkormányzatnál nagy kárt okozó *zsarolóvírus (ransomware)* meg egyenesen szíven üti a felhasználót és a rendszergazdát egyaránt. Mindenki számára világos kell, hogy legyen az is, hogy az *IoT (Internet of Things)* azaz a Dolgok Internete és a *Smart Cities*, azaz az Okos városok, meg az önvezető autók korának hajnalán az információbiztonságot nem lehet félvállról venni.

A világban folyó negatív folyamatok ráadásul szintén kiéleztek bizonyos ellentéteket, amelyek egyre gyakrabban indukálnak a kibertérben folyó támadásokat, csatákat, akár komplett *kiberháborúkat*. A NATO-ra fokozódó nyomás, vagy az Iszlám Állam *kiberterrorista* tevékenysége mellett a nagy zombi hálózatokat irányító hackercsoportok működése is fokozódik. Mindennek köszönhetően nem csak Európa, de az egész világ, az interneten is *„rendpárti"* irányba mozdul el, mind szabályozási, mind gyakorlati szinten.

Az információbiztonság, mint sorvezető

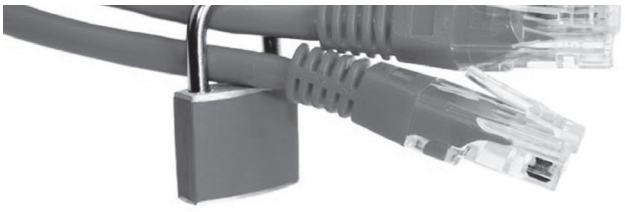
Mindez nagyon rosszul hangzik, de nekünk akár segíthet is az informatikai rendszerünk felélesztésében. Ugyanis az amerikai *NIST* szabványt alapul vevő magyar szabályozás, amellett, hogy szabványhoz/törvényhez illően előír és követel, számos támpontot nyújt a biztonságos működés mellett a hatékony működéshez is. Ez lehet tehát a mi sorvezetőnk.

Ezt a sorvezetőt nem is nagyon kell keresgélnünk. Úgy hívják: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.). Ennek a jogszabálynak az értelmében 2015. június 30-ig valamennyi magyarországi önkormányzatnak (is) rendelkeznie kell működő információbiztonsági rendszerrel, azaz a miénknek is. Hogy milyennel, annak pontos leírása azonban nem ebben a jogszabályban van, hanem a 41/2015. **(VII. 15.)** BM rendeletben (a továbbiakban: BM rendelet), amelynek előd verziója a 77/2013. (XII. 19.) NFM rendelet volt. Ez a rendelet sem túl olvasmányos, cserében viszont nagyon pontosan rögzíti a kereteket, meghatározza a követelményeket, így komoly segítségünkre lehet az informatika felélesztésében és a várható változásokra való alkalmassá tételében. E követelmények egy része fizikai megfelelést követel meg (zónák és azok működésének definiálása, szerverszoba kialakítása, beléptetés működtetése, stb.), másik része a logikai megfelelés feltételeit részletezi (adatmentés, naplózás, vírusvédelem, tűzfal, jogosultsági rendszer, stb.), harmadik

része pedig az adminisztratív (dokumentum alapú) követelményeket ismerteti. Ez utóbbi tartalmazza a teljes biztonsági szabályozás követelményrendszerét és mellette meghatároz több tucat, folyamatos működést leképező *„bizonylatot”*, és az ezekhez kapcsolódó oktatást, belső auditot, karbantartást, stb. fogja össze. A követelményrendszer és a bevezetéssel, működtetéssel kapcsolatos teendők, auditok – és persze kiemelten a képzések – tökéletesen alkalmasak a hivatal dolgozói és vezetői informatikai látásmódjának megváltoztatására, az informatikai kultúra jövőbe tekintő korszerűsítésére – nem beszélve a törvény eredeti céljáról, az információbiztonság valós növeléséről.

Az információbiztonsági rendszer kiépítése

Az IT Biztonság persze nem intézhető el néhány szabályzattal, működése komplex, rendszeres feladatok mellett dokumentációs kötelezettséget is ró az informatikai szakterületre, a jegyzőre és az informatikai biztonsági felelősre (a továbbiakban: IBF), mert folyamatosan működtetni, dokumentálni kell. Természetesen el lehet ezt is nagyolni, de akkor pozitív hatásai helyett csak nyűgöt és kiadást fognak jelenteni. Kísérletet lehet tenni arra, hogy esetleg *„belsőleg”* építsük ki a biztonsági környezetet, s ezzel oldjuk meg az informatika sínre állítását, de gondoljunk csak bele, – a később részletezett kizáró okok mellett – ha eddig nem tudott a szervezet ebbe az irányba menni saját erőből, most vajon mitől fog tudni? Kintről célszerű tehát erősítést kérnünk. Itt is óvakodnunk kell persze az internetről letöltött és átfejlécezett, vagy *„olcsón árult”*, pár dokumentumból álló, uniformizált megoldásoktól, mert azok még látszólagosan és ideiglenesen sem felelnek meg a jogszabálynak, céljainknak és a Hivatallal szemben támasztott elvárásoknak pedig pláne nem.



Az információbiztonsági működtetése

Ha rendszerünket végül kiépítettük, azt működtetni is kell. A bevezetést és a folyamatos működést az IBF felügyeli, akinek a megbízása az Ibtv. és a BM rendelet alapján szintén kötelező Magyarország valamennyi polgármesteri hivatalában, legkésőbb 2015. július 1-től. Az IBF feladata a helyi informatikai munkatárssal együttműködve a biztonsági rendszer kiépítése, üzemeltetése, fejlesztése és az ellenőrzéseken/auditokon való képviselet ellátása, valamint a jogszabályi megfelelés és a jogszabálykövetés garantálása. Az IBF mindezeket a kötelezettségeket, illetve az ehhez tartozó jogokat veszi tehát át a jegyzőtől. Az IBF összeférhetetlenségi és kiválasztási feltételei szintén törvényben meghatározottak. Az IBF jellemzően nem informatikus, feladatai az informatikai eltérő látásmódot igényelnek. Kijelöléséről és megfelelőségről az Ibtv. 13. § (8) és (10) bekezdései rendelkeznek: meghatározott gyakorlat és/vagy végzettség szükséges az ellátásához. Ne bízzuk tehát a feladatot rendszergazdára, mert jellemzően nincs sem végzettsége, sem gyakorlata, sem ideje erre a munkára és még összeférhetetlen is. Ha ő csinálná, olyan lenne, mintha a könyvvizsgálónk lenne egyben a könyvelőnk is. A felelősséget csak olyanra ruházzuk át, aki bizonyítottan szakértője a területnek, mert egyre komolyabb lesz az építmény, amit erre a területre alapozunk. Partnerünktől ne felejtsünk el auditgaranciát kérni! Ha ezt megkaptuk, nyugodtabban fordulhatunk rá az ASP-re, és megerősödve nézhetünk az újabb és újabb elvárások elé.

A következő szint: az ASP

Na, de mi az az annyit emlegetett ASP? Az ASP rövidítés annyit tesz, hogy egy adott alkalmazás az ASP szolgáltató szerverén, azaz egy interneten keresztül biztonságosan elérhető kormányzati felhőben fut, tőlünk távol, nem pedig a hivatalban lévő lokális szerveren, vagy munkaállomáson. (A szakalkalmazások nagyobb része jelenleg is ilyen, csak éppen nem kormányzati, hanem valamely vállalkozás felhőjében futnak.) Az önkormányzati ASP program törekvése fokozatosan egyetlen biztonságos kormányzati felhőbe terelni az egységes szakalkalmazásokat.

Nincs havidíj, nincsenek időrabló riport igények

Gyakran elhangzó kérdés mostanában, hogy miért jó az ASP csatlakozás? Van, aki a veszélyeiről is beszél. Független szakértői körökben az egységes közigazgatási informatika régi törekvés. Szakmailag inkább az a furcsa, hogy eddig húzták a szigetrendszerek, miközben a technológiai feltételek évek óta adottak. Gondoljuk csak bele: ma egyetlen polgármesteri hivatalban 45-55-féle(!) szakrendszer fut, ráadásul minden egyes funkcióra több megoldás létezik a piacon, s így összesen akár 100-200-féle futó szakrendszerről is beszélhetünk országszerte. Ezek megfelelősége, jogszabályi háttere, gyártói támogatása finoman fogalmazva is különböző szintű, esetenként nem is elégséges.

Az önkormányzati ASP szolgáltatásai néhány elterjedt tévhittel szemben nem automatizálnak irodai folyamatokat, bevezetése nem vált ki munkaköröket. Sőt, igen nagymértékben hagyatkozik a helyi felhasználókra, hiszen a rendszer használata csak akkor lehet eredményes, ha tisztított adatokkal, folyamatos és teljes körű adatbevitelen alapszik. Amennyiben a helyi felhasználó ügyintézők bizalmat előlegeznek a rendszernek és a bevezetés nehéz időszakában kellő rugalmasságot tanúsítanak, az üzemszerű működés már komoly előrelépést fog jelenteni a helyi ügyintézés módjában.

Mivel az ASP bevezetése országosan fókuszba helyezi a helyi informatikai fejlesztéseket, minden önkormányzat számára javasolt, hogy elhatározást tegyen az elektronikus ügy-

intézés bevezetése, kiterjesztése mellett is, amelyet az önkormányzati ASP szintén képes támogatni.

Másik nagy előny, hogy az ASP keretében futó rendszereknek nincsen bevezetési díja (sőt támogatást kapunk rá), nincs licencdíja, nem fizetünk használatukért havidíjat, a folyamatos karbantartás és frissítés azonban biztosított. Ez már a gazdálkodás/adó/iktatás szoftvertrió esetében is milliós nagyságrendű megtakarítást jelenthet egy év alatt egy átlagos önkormányzatnál. Ebből a pénzből fokozhatjuk az informatikai biztonságot és többet költhetünk informatikai üzemeltetésre, eszközökre is.

Az Önkormányzati ASP csatlakozás

A 2015-ös Önkormányzati ASP (Application Service Provider, továbbiakban: ASP) pilot projekt után érkezik a kiterjesztett önkormányzati ASP (ASP II.) program, amely a kormányzati szándék szerint 2016-17-ben kötelező érvénnyel fog érinteni majdnem minden önkormányzatot. Tekintettel arra, hogy az önkormányzati ASP távoli szolgáltatásként biztosít szinte minden fontosabb helyi szakrendszert, igénybe vétele egyben fokozza a biztonságosság szintjét, de ugyanakkor sokkal magasabb elvárásokat is támaszt az önkormányzat felé. Talán nyilvánvaló, hogy az ASP-be való belépés egyik alapfeltétele az Ibtv.-nek való teljes megfelelés, révén, hogy a program résztvevőinek minden egyes munkaállomásáról elérhető lesz a kormányzati szerverközpont (felhő). Ez azt jelenti, hogy a felhasználó oldali csatlakozó számítógépek biztonsági kockázatai egyben a kormányzati szolgáltatásra is veszélyt jelenthetnek. Erre tekintettel a csatlakozást támogató felkészülési időszak egyik fontos feladata a helyi biztonsági feltételek megteremtése.

Az ASP II. pályázat

Az ASP II. program indulásával nagyjából egy időben, a KÖFOP éves fejlesztési programja szerint, meg fog jelenni a csatlakozást támogató pályázat is. A pályázat az Ibtv.-nek megfelelő IT biztonsági rendszer fejlesztését is lehetővé fogja tenni (pl. a már kötelezően meglévő 1-es biztonsági szintről 2-es biztonsági szintre lépést), emellett lehetőséget fog adni eszközbeszerzésre és persze a *„nagy feladatra”*, az adatok tisztítására, átmásolására, azaz az adatmigrációra. Az informatikai biztonsági rendszer mielőbbi kiépítésével, továbbléptetésével nagyon sok későbbi kellemetlenségtől óvhatjuk meg magunkat. Természetesen ezen a területen is fontos, hogy képzett, tájékozott és garanciát nyújtó partnert találjunk, aki segíteni fog az ASP előkészítésében is.

A lemaradók esélyei

Mit kockáztatnak azok az önkormányzatok, akik nem az informatika megerősítésében gondolkodnak, hanem tehernek tekintik a biztonságot és veszélyként élik meg a további fejlesztéseket, de legalábbis a halogatás mellett döntenek? Ott, ahol a gyorsuló változásokat látva sem merült fel eddig, hogy a látszaton túl is érdemes lenne a biztonság kérdésével foglalkozni – és sajnos teljesen mindegy, hogy ennek az oka pénzügyi, vagy szakmai kérdés – ott nyilván az informatikának *„nincs szava”*, ott az informatikai infrastruktúra és az informatikai kultúra sincs túl magas szinten. Nos, látva a ránk váró változásokat, nyilvánvalónak látszik, hogy ezek az önkormányzatok sokkal, de sokkal komolyabb problémaként fogják megélni a változásokat, mint azok, akik előrelátóak voltak és túl vannak, de legalább belefogtak informatikai hátterük stabilizálásába eszköz, szabályozási és humán erőforrás területen egyaránt. Ez utóbbiaknak sem lesz könnyű az elkövetkező, fejlesztésektől és változásoktól hemzsegő időszak, de jó háttérrel, sokkal kevésbé lesz megterhelő. Gondoljuk csak bele mi lesz, ha az ASP rendszerelemek telepítésekor derül ki, hogy nincs megbízható informatikusunk, akire számíthatunk, akinek elmondhatják, mi a feladat! Ha akkor derül ki, hogy nincsenek megfelelő eszközeink, hogy nincsenek szabályozva a mentések, nem stimmel a jogtisztaság. Ha ekkor derül ki, hogy a gépeken a dolgozók adminisztrátorként bármit futtathatnak, meg hogy a vírusvédelmünk gyenge, és hogy az operációs rendszereink elavultak… hogy szerverünk sincs… hogy elégtelen a tűzfalunk, meg hasonló anomáliák. Kezdhetünk kapkodni, partnert keresni és gyorsan(!) biztonsági rendszert építeni, eszközöket beszerezni és szabályozási rendszert kialakítani akkor, amikor már az erre épülő szintekkel kellene foglalkoznunk, amikor az új szoftverek oktatásain kellene munkatársainknak ülnie, majd az adatmigrációval kellene foglalkozniuk. Ez olyan lesz, mintha integrálni tanulnánk, miközben nem vagyunk tisztában a szorzás fogalmával és megpróbálnánk a lemaradást még a vizsga előtt tülekedve behozni. Arról nem is beszélve, hogy nem csak mi fogunk későn ébredni, tehát még az sem biztos, hogy lesz egyáltalán, aki „értelmes áron”, vagy bárhogyan megoldja a problémáinkat.

A következő lépés: az elektronikus közszolgáltatások (SZEÜSZ-ök)

A végére maradt még egy izgalmas terület – mert mindent lehet fokozni. Ahogy az várható volt, az államigazgatás más területei után, hamarosan (sejthetően 2017-től) el kell indulnia minden önkormányzatnál valamilyen elektronikus közszolgáltatásnak is, azaz szabályozott elektronikus ügyintézési szolgáltatásnak (SZEÜSZ), legyen az akár csak a bírósági ügyek kezelése, a kutyaoltás, vagy akár az adóegyenleg lekérdezés. A SZEÜSZ-ök elsődleges célja a lakosság elégedettségének növelése, az ügyintézés gyorsítása. Könnyen belátható, hogy ez komolyabb IT biztonsági feltételrendszert kíván, még az ASP-nél is, hisz itt már nem a hivatal képzett dolgozói lépnek be a távoli szerverekre, hanem a lakosok saját otthoni számítógépeikről vagy bárhonnan mobil eszközeikről. Az elektronikus közszolgáltatások elindulása tehát a kockázatok további növekedése miatt minden eddiginél komolyabban fel fogja értékelni az informatikai biztonság területét. Ezen kockázatok kezelése pedig a jegyző hatásköre…

A közeljövő utáni nem túl távoli jövő

De még mindig nincs vége. Az építést normális esetben megelőzi a tervezés fázisa. A tervezéskor általában előre szoktunk tekinteni, hogy ne tervezzünk olyat, amit később, újabb tervek miatt le kell bontani, vagy alapvetően meg kell változtatni. Ez persze könnyebb, ha látjuk a trendeket, ha vannak előttünk minták. Nos, esetünkben vannak. Ezek a minták, példák, tervek egységesen a Smart City, az élhetőbb, szerethetőbb, fenntartható *„okosváros”*, okos település megvalósulása felé mutatnak. Persze ennek az alapja is az informatika.

A Lechner Tudásközpont Nonprofit Kft., mint a téma kormányzati felelőse, az okos városok kialakítására vonatkozóan négyféle célt határoz meg. Smart City építésénél cél

- a szolgáltatások minőségének javítása,
- az erőforrás-felhasználás hatékonyságának növelése,
- a társadalmi részvétel, partnerség, befektetések, civil összefogások szerepének növekedése a települési szolgáltatások körében
- és persze a fejlett szolgáltatások fenntarthatóságának megteremtése.

Ezen szempontok mentén érdemes, szabad, okos várost tervezni.

Az okos városok tervezésének, kiépítésének és működtetésének mára hatalmas irodalma van. A tapasztalatok, az eredmények elérhetőek. Rengeteg követendő és persze elkerülendő mintánk van.

Mit tudhat a Smart City?

A Brit Szabványügyi Hivatal definíciója szerint az okos város olyan település, *„ahol megvalósul a fizikai, a digitális és a humán rendszerek hatékony integrációja az épített környezetben hogy fenntartható, prosperáló és inkluzív jövőt biztosítson lakóinak”*.

A Smart Cityről az embereknek általában annak egyes elemei jutnak eszébe. Olyanok, mint pl. a digitális közigazgatás, az intelligens kamerákkal megerősített közbiztonság, a szociális és időskori ellátásban alkalmazott okos karkötő, a városüzemeltetés térinformatikai támogatása, a kátyúregiszter, vagy a faregiszter, az okos közlekedési lámpák, a közvilágítás okosítása, a turizmust támogató különféle megoldások, a közterületi wifi, az okos és zöld középületek, irodák hivatalok, könyvtárak, a távfelügyelt, okos közművek, ilyesmik. Mindez megint csak a modern informatika vívmánya, azaz újra oda lyukadunk ki, hogy a trendek egy irányba mutatnak, az informatikai kultúra kialakításának, fejlesztésének szükségessége és általában véve az informatika gondolkodásunkba való beépítése irányába.

Persze ez leegyszerűsítés. A Smart City ugyanis nem csak informatika. Hat nagy területe *1.* az okos mobilitás (smart mobility), *2.* az okos, élhető környezet (smart environment), *3.* az okos polgár (smart people), *4.* az okos életkörülmények, életminőség (smart living), *5.* az okos kormányzás (smart governance) és *6.* az okos gazdaság (smart ecomomy). Már a területek elnevezésekből is látszik, hogy a Smart City nem egyszerűen a környezet digitalizálásáról szól, de még csak nem is egyszerűen arról, hogy informatikai eszközökkel jobbá tesszük az életet. Magyarul nem csak informatikai, annál több: másféle szemléletváltásról is szól. A digitális közigazgatás pl. sokkal nagyobb előrelépést jelent, ha nem egyszerűen *„áttesszük internetre a valahogyan eddig működő folyamatot”*, hanem újra átgondoljuk, újra szervezzük, hatékonyabbá tesszük figyelembe véve a korszerű rendeket, mintákat (környezetvédelem, energiahatékonyság, fenntarthatóság, stb.). Az okos város egyik alapvető eszköze, de csak eszköze, tehát az informatika.

A szakadék átugrása

Mondhatjuk ugye, hogy messzire jutottunk gondolatban? Azonban időben nem. Nyugaton máris kitűnő, működő példák akadnak. Magyarország bizonyos települései (mondjuk Miskolc vagy Ceglédbercel), már szintén elindultak a Smart City felé vezető úton. A kezdeti lépéseket már több helyen megtették és legalább a tervezés szintjén állnak. A háttérbe szorított hivatali informatikával a jövő okos városába bizony nagyot kell ugrani. Az részmunkaidős informatikus bérével, és az eszközpark korszerűsítésével, való spórolással szemben a szakadék másik oldalán a Smart City tervezését és megvalósítását felügyelő településfejlesztési szakemberek, mérnökök, információbiztonsági szakemberek és elégedett polgárok állnak. Gondolkodásunk homlokterébe lassan átkerül az IT. Ez talán már nem is paradigmaváltás, hanem *„életmód”*. A jövő elkezdődött. Mielőbb be kell lépnünk a kapuján! Nem nagyon van hová hátrálni, mert ez nem csak a Hivatalra igaz, hanem a szűk és a tág otthonunkra is.

Használt fogalmak és megemlített személyek

ASSANGE, Julian

Ausztrál újságíró, internetes aktivista, korábban programozó és hacker. A WikiLeaks főszerkesztőjeként és szóvivője – ma tanácsadója. Nem publikus források felhasználásával számtalan, kiszivárogtatott jogsértést leleplező dokumentumot tett közé a WikiLeaks oldalain.

ASP

Application Service Provider, azaz Alkalmazás szolgáltató, akinek a távoli infrastruktúráját igénybe vesszük bizonyos alkalmazások futtatásához.

BSI

British Standard Institution, azaz a Brit Szabványügyi Intézet. A NIST-hez és az ISO-hoz brit nemzeti hasonló szabványkibocsátó és fejlesztő szervezet.

cloud

Jelentése felhő. Adataink tárolására, rendszereink futtatására igénybe vehetünk távoli tárhelyet, futtatási környezetet. Ilyenkor egy szolgáltató valamely távoli szerverparkban lévő eszközein tárolódnak az adataik, vagy futnak alkalmazásaink, nem a mi asztali gépünkön, vagy lokális szerverünkön.

DDoS

Distributed Denial of Service, azaz túlterheléses támadás. Sok-sok *„zombi gép”* kérésekkel áraszt el egy szervert, ami leterhelődik emiatt és elérhetetlenné válik.

felhő

Lásd cloud!

hacker

Olyan számítógépes szakemberek, akik általában tudásukkal visszaélve, jogosulatlanul számítógépbe illetve számítógép-hálózatokba törnek be haszonszerzés vagy károkozás céljából. Az *„etikus hackerek”*, ugyanezt a védelem gyenge pontjainak felderítése céljából, általában a rendszer tulajdonosának megbízásából végzik.

IBF

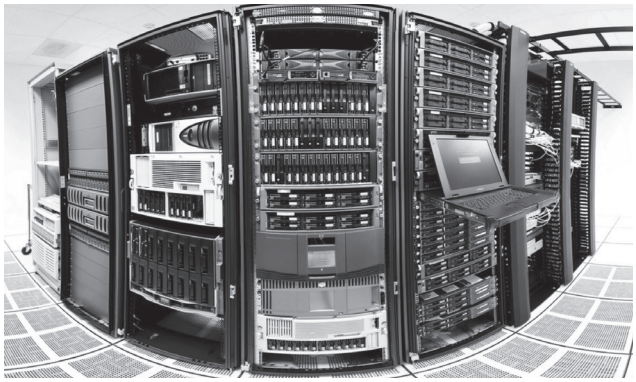
Információbiztonsági felelős. Az informatikai rendszer biztonságáért felelős, kinevezett személy, aki otthon van mind a jogi szabályozás, mind az elektronikus információs rendszerek üzemeltetése, mind az információbiztonság terén. Az IBF a rendszergazdával együttműködve kialakítja, működteti és fejleszti az informatikai rendszert, kiemelt prioritásként kezelve a biztonsági szempontokat, kialakítva a fizikai, a logikai és az adminisztratív biztonságot.

iCloud

Az Apple felhőszolgáltatása, azaz távoli szerverein tárolt adatok helye, ahonnan a privát, erotikus celeb képek kikerültek a szabad internetre.

IoT

A dolgok internete, vagyis az IoT (Internet of Things) a következő forradalom alapja. Az interneten keresztül egymással és különböző szolgáltató központokkal kommunikáló eszközökből, épületekben, lakásokban, termelő üzemekben, szolgáltató központokban, vagy az utcán, közlekedési eszközökben és az emberi testen, elhelyezett mobil érzékelőkből, szenzorokból álló hálózat, melynek működése során összegyűjtött információk alapján forradalmi megoldások és szolgáltatások fogják megkönnyíteni az életünket és megsokszorozni az információbiztonság jelentőségét.



kibertér

Számítógépes hálózatok összessége, azaz az internet teljessége. *„A kibertér (angol: cyberspace) számítógép-rendszerek és -hálózatok által alkotott metaforikus tér, amelyben elektronikus adatok tárolódnak és online adatforgalom, valamint kommunikáció zajlik.”* (forrás: Wikipedia.hu)

kibertámadás

A kibertéren keresztül indított támadás, amely a megtámadott eszköz, vagy hálózat feletti ellenőrzés átvételére, működésének ellehetetlenítésére, vagy a tárolt adatok megszerzésére irányul.

kiberterrorizmus

Kifejezetten romboló szándékú kibertámadás, amelynek célja a megtámadott rendszer működésének ellehetetlenítése, vagy akár fizikai elpusztítása.

kiberháború

Nagyobb, független, vagy állami hackercsoportok egymás infrastruktúrája ellen indított, összehangolt, elhúzódó kibertámadás sorozata. Előfordul államok között is. Néha nem is azonosíthatók a szereplői.

malware

Malicious Software, azaz kártékony szoftver kifejezés rövidítése. A kártevő alkalmazások (vírusok, kémprogramok, kéretlen reklámok, stb.) gyűjtőneve.

NAS

Network Access Storage, azaz hálózati elérésű tároló. Olyan *„szerver”*, amelynek nincs billentyűzete, sem monitora, hanem a hálózaton keresztül rácsatlakozva egy másik eszközről: számítógépről, okos telefonról, stb. érjük el. Igazi céleszköz. Egyedi operációs rendszere van, amely a nagyon drága szerver operációs rendszerekkel szemben eleve benne van az eszköz árában, viszont azokhoz képest korlátozott funkcionalitást tesz lehetővé. Kisebb hálózatokban állományok közös elérésére, tárolására, adatmentésre, archiválásra használjuk. Előnye az alacsony ár és a stabil működés. Hátránya a korlátozott funkcionalitás.

NIST

A National Institute of Standards and Technology, azaz a Nemzeti Szabvány és Technológiai Intézet, az amerikai Kereskedelmi Minisztérium egyik részlege, amely laboratóriumok sokaságát működteti. A NIST SP 800 IT Security szabványa az alapja a BM rendeletnek.

ransomware

A ransomware, magyarul zsarolóvírus egy olyan kártékony szoftver (malware), amely lezárja a felhasználó fájljait, méghozzá gyakorlatilag a visszaállítás lehetősége nélkül. Fajtától függően blokkolja az áldozat hozzáférését a számítógéphez és az okozott károk visszafordításáért minden esetben váltságdíjat követel. A váltságdíj összege az adott vírus típustól függ, de többnyire több tíz illetve százezer forintnak megfelelő Bitcoin. A zsarolóvírusok, sok más malware-hez hasonlóan, képesek lehetnek az áldozat érzékeny személyes adatainak megszerzésére (jelszavak, banki belépési adatok), a védelmi szoftverek (antivírus, Anti-Spyware stb.) leállítására, megtévesztő figyelmeztetések megjelenítésére és más kéretlen tevékenységekre is. (forrás: ransomware.hu)

Smart City

Okos város. Ahol megvalósul a fizikai, a digitális és a humán rendszerek hatékony integrációja az épített környezetben hogy fenntartható, prosperáló és inkluzív jövőt biztosítson lakóinak. (forrás: BSI)

SNOWDEN, Edward

Az amerikai Nemzetbiztonsági Ügynökség (NSA) volt vezető tanácsadója, aki nyilvánosságra hozott szigorúan titkos dokumentumokat, amelyekből kiderül, hogy az amerikai titkosszolgálatok széles körben figyelik az emberek mobiltelefon-hívásait és internetes tevékenységét az Egyesült Államokban és világszerte. (forrás: Wikipedia.hu)

SZEÜSZ

A SZEÜSZ-ök, a szabályozott elektronikus ügyintézési szolgáltatások. Magyarán az ügyintézés internetes platformra való áthelyezése. Elsődleges célja a lakosság elégedettségének növelése, az ügyintézés gyorsítása.

térinformatika

Angolul GIS – Geographical Information Systems. A körülöttünk lévő térbeli objektumok és jelenségek elhelyezkedését informatikai eszközökkel rögzítő és elemző tudományterület. Pl. fa- és bokor regiszter – adott területen lévő fák és bokrok elhelyezkedésének és egyéb adatainak a regisztere.

wifi

Viszonylag kis hatókörű, vezeték nélküli mikrohullámú kommunikációt (WLAN) megvalósító, széleskörűen elterjedt szabvány alapján működő helyi (irodai, otthoni, közintézményi, szabadtéri) helyi hálózat.

WikiLeaks

A WikiLeaks egy nemzetközi nonprofit szervezet, amely kiszivárogtatott kormányzati és egyéb dokumentumokat publikál az Interneten, miközben forrásainak névtelenséget biztosít. (forrás: wikipedia.hu)

zombi számítógép, zombi hálózat

A zombi számítógép olyan gép, amely felett illetéktelenek átvették az irányítást vírusokkal és/vagy trójai szoftverekkel. A számítógép erőforrásait ezután a saját céljára, gyakran DDoS-támadások során használják fel. A zombi hálózatokba (botNet) kapcsolt számítógépek százaival hatalmas károkat okoznak a megtámadott intézményeknek, szervezeteknek, államoknak, vállalatoknak.

zsarolóvírus

Lásd ransomware!