Debreceni Egyetem
Informatika Kar

INFORMÁCIÓMENEDZSMENT
Adatvédelem, adatbiztonság

Témavezető:
Dr. Kormos János
egyetemi tanár

Készítette:
Seres Viktória
gazdaságinformatikusBSc

Debrecen
2010

Szeretnék köszönetet mondani témavezetőmnek, ***Dr. Kormos János*** Tanár Úrnak szakdolgozatom elkészítésében nyújtott segítségéért és útmutató tanácsaiért.

„Szerezz olyan vagyont, amelyet a tolvajok nem tudnak ellopni, melyhez nem férhetnek hozzá a zsarnokok, amely halálod után is megmarad, sohasem lesz kevesebb és sohasem enyészik el.”

[hindu bölcsesség]

Tartalomjegyzék

1. Bevezetés

Témakörömnek az *Információmenedzsment*et választottam, ezen belül az *adatvédelemmel és az adatbiztonság*gal foglalkozok.

Az elmúlt 20 évben jelentős változásoknak lehettünk szemtanúi és ez a változás a mai napig tart. A számítástechnika és az Internet térhódítása, megváltoztatta mindennapi életünket. Nem csak a szabadidős tevékenységeinket, de a munkafolyamatokat is jelentősen befolyásolja. Ma már elképzelhetetlennek tűnik, hogy egy vállalat a modernkor vívmányait ne használja, a számítógépen rögzítik, dolgozzák fel és elemzik az adatokat. Az információmenedzsment ennek a változásnak köszönheti fellendülését, mivel az információmenedzsmenthez tartozik a vállalaton belül minden, ami az információkkal és a számítástechnikai eszközökkel kapcsolatban áll. Szakdolgozatomban az adatvédelemmel és adatbiztonsággal foglalkozok részletesebben. Fontos, hogy naprakészek legyünk az adatvédelem területével kapcsolatosan mivel, ha elhanyagoljuk a vállalatnak ezt a részét, akkor könnyen valamilyen rosszakaró áldozatai lehetünk.

Az első részt, a számítógép és az Internet rövid történeti áttekintésével kezdem, nem tehetem meg, hogy ne ismertessem a fontosabb állomásokat, mivel ezen eszközök képezik az információmenedzsment alapjait. Ezek után az információmenedzsment területének alapvető definícióit ismertetem, amiből kiderül, hogy hogyan épül fel az információ és a tudás. Milyen kapcsolat van a jel, adat, információ és tudás között és kiderül az is, hogy mi is az a tudáspiramis és hogyan épül fel. Ebben a fejezetben foglalkozok az információmenedzsment területével részletesebben. Próbálok egy pontos definíciót meghatározni, mivel nincs egységesen megfogalmazott mindenki számára elfogadott fogalma. Az IM szervezeten belüli céljaira és feladataira is kitérek, miért előnyös IM eszközöket alkalmazni a vállalatok számára.

A második részben, az információmenedzsmenten belül az adatvédelem témakörével foglalkozok. Ismertetem az adatvédelem, adatbiztonság fogalmát és az ezek közötti különbségeket. A vállalatokra leselkedő főbb veszélyekkel is foglalkozom, többek között, a véletlen és szándékos emberi károkozással, időjárási katasztrófákkal és kitérek arra is, hogy ezeket a veszélyeket hogyan lehet kikerülni, csökkenteni a bekövetkezésüknek valószínűségét. Fontosnak tartom, hogy az adatvédelem jogi hátterét is ismertessem és ezen

belül is a magyarországi adatvédelmi jogalkotást. A vállalatoknak az információ vesztés elkerülése érdekében, fel kell készülniük a váratlan eseményekre is, ennek érdekében egy megfelelő kockázatelemzést kell végrehajtani. Szakdolgozatomban elmondom, hogy a kockázatelemzés készítése során mikre kell oda figyelni, minden lehetséges esetet meg kell vizsgálni annak érdekében, hogy eredményes legyen a vizsgálódás. Ha a szervezeten belül a kockázatelemzést részletesen végig gondolták és kielemezték, akkor ezután a katasztrófa-elhárítási tervek megalkotása következik, itt leírom, hogy a katasztrófa-elhárítási tervet, hogyan kell felépíteni, költség és védelem szempontjából hatékonyan, ismertetem a katasztrófa-elhárítás különböző alapváltozatait is.

A következő részben az adatbiztonságról írok, ez is szorosan kapcsolódik az adatvédelemhez. Az adatbiztonság az adatvédelem szűkebb részét képezi, mivel nem globálisan a vállalat egész rendszerének védelmével foglalkozik, hanem csak az adott dokumentumokkal. Elmondom, hogy miért fontos az adatbiztonság, milyen titkosítási módszereket használhatunk, az egy és két kulcsos titkosítási módszereket ismertetem, alkalmazásukat, lépésről lépésre a titkosításuk folyamatát is feltárom. Ezek után elmondom, a különböző támadási formákat, hogy hogyan juthatnak a támadók a titkosított adatainkhoz. A következő pontban a vállalaton belüli partner-azonosítással foglalkozom. A biometrikus, a tudás és a birtok alapú azonosításról is esik néhány szó és elmondok egy-egy példát is. A biometrikusnál az ujjlenyomat-olvasót, a tudásalapúnál, pedig a jelszó használatát ismertetem. A jelszavaknál elmondom, hogy mennyire biztonságos az alkalmazása, a különböző karakterek használatával milyen valószínűséggel törhetőek fel a jelszavak. A különböző azonosítási módszerek sajátosságait is foglalkozom, hogy hol lehet jól alkalmazni az egyes fajtákat, mik az előnyeik és hátrányaik. A partner-azonosítás után a digitális aláírással foglalkozok. Mindennapjainkban fontos szerepet tölt be, mivel ezáltal a világ bármely pontján lévő partnerrel köthetünk üzletet anélkül, hogy bárkinek is több száz kilométert kellene utazni. Az Internet elterjedésének köszönhetően már nem csak üzleti ügyeinket, hanem személyes ügyeinket is intézhetjük a hálózaton keresztül. A digitális aláírás hiteles alkalmazásához, azonban a tanúsítvány ismerete is szükséges, ennek az eszköznek a feladata, hogy a nyilvános kulcsot egy megbízható harmadik fél segítségével hitelesítse, akinek a segítségével megbizonyosodhatunk arról, hogy a digitális aláírás tényleg azé, aki küldte.

Az *Információmenedzsment Adatvédelem, adatbiztonság* című szakdolgozatom megírásának célja az volt, hogy ismertessem, hogy milyen lehetőségeket rejt az

információmenedzsment területe és ezt a területet érintő veszélyekre akartam felhívni a figyelmet és a lehetséges védekezési módokat is taglaltam, annak érdekében, hogy védelmi rendszerünk, minél hatékonyabb legyen. Próbáltam tanácsokat adni annak érdekében, hogy a különböző problémákat, hogyan lehet a legmegfelelőbben elkerülni vagy megoldani.

2. Információmenedzsment

2.1. Történeti áttekintés

A következő néhány sorban, a teljesség igénye nélkül, a számítógép és az Internet történetének legfontosabb állomásaival fogok foglalkozni. Fontosnak tartom, hogy ezekről is essen néhány szó, mivel nélkülük a világ fejlődése nem tartana ott, ahol napjainkban tart.

Ezen eszközök hiányában az én szakdolgozatom se született volna meg, mivel az információmenedzsment a számítógépes folyamatok révén könnyíti meg a szervezetek működésének mindennapjait. A vállalatok életében is mindennapossá vált a számítógép használat. Elképzelhetetlen lenne ma már, hogy a vállalatok információ-technológiai eszközök nélkül tudjon létezni, mivel ezeken az eszközökön rögzítik és dolgozzák fel az információkat.

2.1.1. Számítógép története

A számítástechnika története az ENIAC-kal (Electronic Numerical Integrator And Computer) vette kezdetét. Ez volt az első nagy mérföldkő az informatika történetében. Az ENIAC tervezését hadászati célokkal a második világháború alatt kezdték el, a Pennsylvania egyetemen. John Presper Mauchly és John William Eckert 1946-ban fejezték be a megépítését. Az ENIAC hihetetlen méretekkel rendelkezett, kb. 17 500 elektroncsőből épült fel, 30 tonnát nyomott és 150 négyzetméternyi területet foglalt el. Ez volt az első programozható, elektronikus számítógép, mintegy kétnapos munkába tellett, mire átprogramozták egyik folyamatról a másikra. Az összeadást 0,0002 másodperc alatt, a szorzást, pedig 0,003 másodperc alatt tudta elvégezni. Tízes számrendszerben működött, memóriája 20 db tízjegyű előjeles számot kezelt. Fő feladata ballisztikai táblázatok készítése volt. Ma már egy egyszerű számológép is nagyobb teljesítményű, mint az ENIAC volt, de

ettől függetlenül, a történelemben hasonló jelentőséggel bír, mint az autó vagy a tévé feltalálása.

Az ENIAC feltalálása után a fejlődés gyorsult. Az elektroncsöveket a tranzisztorok váltották fel. A méretek jelentősen csökkentek, a teljesítmény és a megbízhatóság, pedig fokozatosan növekedett. Másodpercenként már egymillió művelet elvégzésére voltak képesek a számítógépek. Sokkal kevesebb energiát használtak fel és sokkal hosszabb életűek lettek. A méretcsökkenésnek, a hosszabb élettartamnak és olcsóbbá válásának köszönhetően a számítógépek, egyre több helyen jelentek meg (kutatóintézetek, egyetemek). Ezeknek a fejlődéseknek köszönhetően egyre több vállalat látott lehetőséget a számítástechnika területében, ezért egyre többen kezdtek el számítógépekkel és ezek alkatrészeivel foglalkozni (például gyártás).

A következő nagy állomás a mikroprocesszorok megjelenése volt. Ezeknek az eszközöknek köszönhetjük, hogy a számítógépek teljesítménye, sebessége is tovább növekedett. 1969-ben az Intel kezdte el az első mikroprocesszor megépítését, 1971-ben fejezte be, az úgynevezett Intel 4004-esét. 2300, szilíciumalapú tranzisztorból állt, a teljesítménye az ENIAC-kal egyezett meg. Utasításkészlete 45 utasításból állt. Kezdetben a mikroprocesszorokat jelzőlámpák, automata mosógépek, vérmintaelemző gépek vagy űrszonda vezérlésénél használták fel, a jelentős költséghatékonysága miatt. A mikroprocesszorok tranzisztorainak száma 1,5- 2 évente a duplájára növekszik, teljesítménye jelentősen nő.

A személyi számítógépek történetében az áttörést Micro Instrumentation Telemetry Systems (MITS) cég hozta az Altair 8800-as csomaggal, amelyet a felhasználóknak kellett összeszerelniük. Nem várt sikereket hozott az első személyi számítógép, több tízezer darabot adtak el belőle. A billentyűzetet egy kapcsolótábla, a képernyőt, pedig néhány sor, világító dióda helyettesítette és ezek mutatták az információkat. Kezdetben csak gépi kódolással, majd Paul Allen-nek és Bill Gates-nek köszönhetően BASIC-ben is programozhatóvá vált az Altair 8800-as.

A Tandy Corporation 1977-től kezdte el árusítani, azokat a számítógépeket, amelyek katódsugárcsöves képernyővel és billentyűzettel is rendelkeztek már. A gép népszerűségét az is növelte, hogy programozni lehetett és a felhasználók az információkat mágneskazettákon tudták tárolni.

Innentől már egyenes út vezetett ahhoz, hogy a legtöbb ember számára a számítógép mindennapjai részévé váljon.

2.1.2. Internet története

Az Internet története az 1960-as években kezdődött. Ez is, mint oly sok dolog (például: számítógép), hadászati kutatásoknak köszönhetően jött létre. Az Amerikai Egyesült Államok végzett kutatásokat, azzal kapcsolatban, hogy hogyan tudnának létrehozni egy olyan információs rendszert, amelynek segítségével egy esetleges katasztrófa vagy bombatámadás esetén is az USA fontosabb bázisai kapcsolatban tudnának maradni egymással és Amerika így nem maradna védtelen.

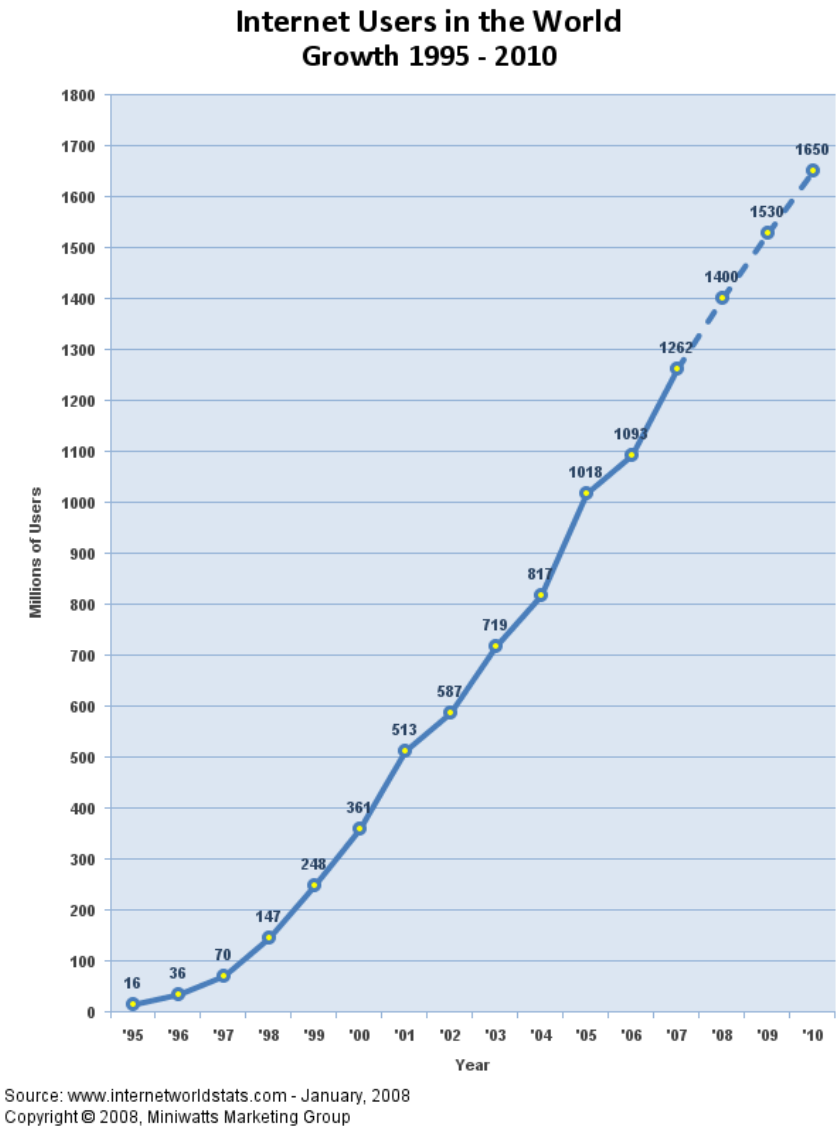
1969-ben az USA Hadügyminisztériuma kísérleti jelleggel létrehozott, telefonvonalon keresztül egy csomagkapcsolt hálózatot, amely az ARPAnet (Advanced Research Projects Agency NETwork) nevet kapta. Ezt a hálózatot úgy alakították ki, hogy decentralizált legyen, ne legyen egyetlen kitüntetett központja, mert az első támadások célpontja ez a központ lenne, hanem mindegyik állomás, hasonló jogkörökkel rendelkezzen. Bármikor szabadon alakíthatónak fejlesztették ki, ha esetleg megsérül, megsemmisül egy központ (a hálózattal való összeköttetése, így megszakadt), vagy ha újabb központot csatlakoztatnak a hálózathoz, akkor is zavartalanul tud működni az egész rendszer. A hálózatban részt vevő elemek egymással elektronikus leveleket válthattak, távolról bejelentkezhettek egymás számítógépeire és a távoli adatbázisaikat is könnyen elérhették, ezért nem csak háború idején, hanem a békesség idején is nagy hasznát vették az USA-ban. Ez a csomagkapcsolt, többközpontú kommunikációs rendszer a TCP/IP őse.

Az első bekapcsolásra 1969. szeptember 2-án került sor, de a tényleges hálózaton keresztül történő adatcserére még két hónapot várni kellett, mivel a Stanford egyetem csak addigra tudott csatlakozni a hálózathoz. A folyamat nem állt meg itt. Az elkövetkező hónapokban további három intézmény is csatlakozott, a Stanford Research Institute (SRI), a University of Utah, valamint a Santa Barbara-i Egyetem (UCSB) is. Majd az évek során egyre több amerikai egyetem kezdett rákapcsolódni az Internet elődjére. A 70-es évek közepétől kezdve a hálózatnak már külföldi csomópontjai is léteztek, és az ARPANET hamarosan a ma is ismert, az egész világot behálózó Internetté alakult át. [9]

Az ARPANET-et 1983-ban, két részre osztották, egyrészt, megmaradt a szigorúan ellenőrzött hadászati rész, ez lett a MILNET, másrészt létrejött a mai szóhasználatunkban használt Internet. A National Science Foundation (NSF) felismerte, hogy a tudományos életben milyen nagy lehetőségeket rejthet ez a hálózat, ezért jelentős fejlesztésekbe kezdett. 6 szuperszámítógépet kapcsoltak az ARPANET hálózatához 1985-1986-ban, ez a hálózat NSFNET nevet kapta. A hálózatot optikai kábelekkel hozták létre, az Amerikai Egyesült Államokban a mai napig az Internet gerinchálózatát adja. Az NSFNET hálózat után, sorra jöttek létre a különböző hálózatok kezdetben mindenki az NSFNET -hez akart csatlakozni, de gyakran egymással is kapcsolatokat hoztak létre. Így alakult ki a mai szerteágazó, óriási, átláthatatlan Internetes hálózat.

Az Internet fejlődésének következő jelentős lépése 1989-ben következett be. A genfi Európai Részecskefizikai Laboratórium (CERN: Conseil Europeen pour la Recherche Nucheaire) munkatársai, Tim Berners-Lee és Robert Cailliau vezette csoport, készítette el azt az interaktív dokumentumkezelő rendszert, amely a beépített kapcsolatokat (hyperlink-ek) segítségével az összefüggő információkat a felhasználó számára egyszerű módon hozzáférhetővé tette az Internet bármely pontjáról. 1993 áprilisában az Illinois Egyetem néhány diákja elkészítette az első grafikus kezelőfelülettel rendelkező böngészőt a Mosaic-ot, amely nem csak a kutatók, hanem a laikusok számára is könnyen kezelhetővé tette az Internetet. [3]

Ettől kezdve az Internetet használók száma rohamosan emelkedett, ez az emelkedés napjainkban se lassul. Évente kb. 150 millióval növekszik, négy évente pedig megduplázódik az Internet használók száma, ezt mutatja az 1. ábra is.



1. ábra: Internet felhasználók számának növekedése

2.2. Jel, adat, információ, tudás

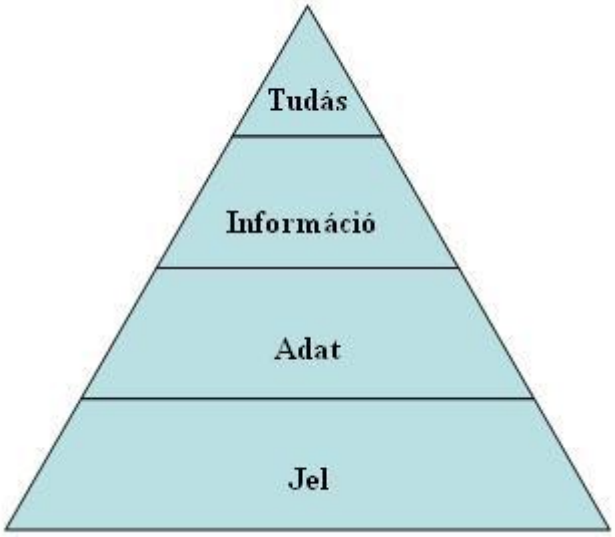
A *jel* olyan jelenség, esemény, amely önmagán túlmutat és általa valaminek a meglétére, bekövetkeztére, okára következtethetünk. A 2. ábrán látható, hogy a jel a tudáspiramis legalján helyezkedik el, ezek összefüggéstelen adatelemek. A jelek önálló jelentéssel nem bírnak. Jeleknek nevezzük a különböző karaktereket, mint például a betűket, számokat, különleges karaktereket. A jelek összességét jelkészletnek nevezzük.

„Az *adat* olyan szimbólum vagy jelsorozat, amely esetleges későbbi felhasználás céljából, a működő környezetben végbemenő változásokat, meglévő állapotok egyes jellemzőit továbbításra és megőrzésre alkalmas formában rögzíti.”[5] Az adatok önmagukban nem rendelkeznek jelentéssel. Az adatok jelekből épülnek fel, különböző feldolgozási folyamatok révén nyernek értelmet, az adatokból így keletkezik az információ.

„Az *információ* olyan tájékozódás, közlés, adat, ismeret, hír, amely a címzett által értelmezhető, és amelynek célja a bizonytalanság csökkentése, a lehetséges alternatívák közötti döntés elősegítése.” [5] Az információ mindig valamilyen új ismeretet hordoz és értékét attól, függően határozzuk meg, hogy az információ tartalma milyen pontos, mennyire fontos számunkra, a forrása mennyire hiteles. Ezek a jellemzők befolyásolják azt, hogy milyen szinten védendők az információk, mennyi energiát (pénz, idő, munka) érdemes arra fordítani, hogy ne juthasson illetéktelen kezekbe és ne tudjanak visszaélni az adott információval. Az információk a vállalatok működésének alapkövei. A szakdolgozatom 3. és 4. részében részletesebben foglalkozok az információk védelmének témakörével, azzal hogy hogyan lehet egy vállalaton belül megvédeni hatékonyan az értékeket, mind a jogosulatlan hozzáférésektől, a módosításoktól, a törlésektől, a nyilvánosságra hozataltól és az egyéb károktól.

„A *tudás* a valós világnak, az abban létező dolgoknak, tényeknek, eseményeknek, jelenségeknek, az azok között fennálló kapcsolatoknak, ok-okozati összefüggéseknek az emberi tudatban történő visszatükröződése.” [5] A tudáspiramis legfelső szintjén helyezkedik el. Az információk közötti ok-okozati összefüggések meglátásával egy magasabb szintre jutunk, a tudás megszerzéséhez. Tudást tanulás és tapasztalás révén szerezhetünk. Az információ tudássá alakítása az egyén, egyének feladata.

A jel, adat, információ és tudás közötti kapcsolatot, legegyszerűbben egy piramis alakú grafikonon ábrázolhatjuk, ezt a 2. ábra szemlélteti.



2. ábra: Tudáspiramis

2.3. Információmenedzsment

Az információmenedzsment a 80-as évek végén, a 90-es évek elején kezdte meg hódító útját a vállalatok életében. Ez többek között az Internet használatának leegyszerűsödésének és a különböző irodai programcsomagok megjelenésének volt köszönhető, mivel az információmenedzsment feladata többek között, a megfelelő minőségű adatok gyűjtése, erre a legegyszerűbb megoldást az Internet nyújtja, és az adatok feldolgozása a feladata, ezt pedig legkönnyebben a programcsomagok segítségével lehet megoldani, mivel ezeket a szoftvereket kifejezetten arra fejlesztették ki, hogy megkönnyítsék egy-egy vállalat életét. Az Információmenedzsment lehetővé teszi, hogy a leggyorsabban és a legegyszerűbben juttassa a vállalatot a megfelelő adatokhoz, a különböző informatikai eszközök segítségével.

Ez a tudományág folyamatosan változik, fejlődik a számítástechnikának és az informatikai eszközök fejlődésének köszönhetően. Az információmenedzsmenttel foglalkozó szakembert, információmenedzsernek nevezzük, akinek a feladata az információval, mint erőforrással foglalkozni.

Fogalom meghatározása: [16]

Az információmenedzsmentnek nincs egyértelműen megfogalmazott és elfogadott definíciója, ezért az információmenedzsment területén foglalatoskodó néhány szakember megfogalmazását vizsgálom:

„A szervezet (belső/külső) információs erőforrásainak menedzselésével foglalkozik, biztosítva az elvárható hatékonyságot az információs folyamatokban. Az IM szerep lényege és specifikuma a fenti követelmények alapján a hatékony vállalati, szervezeti információáramlás menedzselése.” Dobay Péter

„Az információmenedzsment a vállalat szakmai vezetésével szorosan együttműködve felelős az információrendszerek szervezésére, tervezésére, működtetésére és irányítására szolgáló tevékenységek elvégzéséért, a feltételek biztosításáért, küldetése és feladata tehát a szervezet céljaival szoros összhangban lévő, annak működését leghatékonyabban támogató információrendszer kifejlesztése, működtetése és a működés ellenőrzése” [5]

„Az információmenedzsment bármely szervezetben lévő információs források hatékony kezelésével és összehangolásával foglalkozik.” Mikulás Gábor

„Bonyolult, integrált rendszerek esetén nem közömbös, hogyan találnak egymásra a fogyasztók (a felhasználók) és a termékek (az információsrendszer szolgáltatásai). Azt a tevékenységet, amely hidat képez a felhasználók és a szolgáltatások között, nevezik információmenedzsmentnek.” [3]

Az információmenedzsment fogalmát a szakemberek különböző szempontok alapján közelítették meg, attól függően, hogy mely folyamatokban vesznek részt az információmenedzsment területén belül, mely részek a mérvadók a munkájuk során, de mind a négy megfogalmazásból kiderül, hogy az információmenedzsment a szervezetek számára nyújt segítséget az információ gyűjtésében, feldolgozásban. Elmondhatjuk, hogy az információmenedzsment a szervezet sikeres működéséhez szükséges adatokat, információkat, tényeket biztosítja, feldolgozza az információkat annak megfelelően, hogy mire szeretnék felhasználni, majd ezeket a szervezet megfelelő részeire továbbítja és tárolja.

Az információmenedzsment feladata és célja:

Az információmenedzsment célja, hogy az információkat maximálisan felhasználhatóvá tegye. Az információmenedzsment feladatához tartozik minden olyan tevékenység, amely az információval és a számítógéppel összefüggésbe hozható, vagyis ide

tartozik a megfelelő minőségű adatok gyűjtése, feldolgozása, értékelése, tárolása, a visszakeresés, a hozzáférhetőség, a megfelelő jogszabályok betartása.

Az információmenedzselés legfontosabb teendője az, hogy jó minőségű információkat nyújtson a vállalat különböző területeinek. Úgy dönthetjük el, hogy az adott információ jó minőségű volt-e, hogy az adatokat megvizsgáljuk, az adott információ felhasználásával és felhasználása nélkül megnézzük, milyen döntési folyamatot választanánk, ha ugyanazt a döntési folyamatot végeznénk el, akkor a megszerzett információnak az értéke nulla. Mivel a megszerzett információnak az a feladata, hogy a döntési bizonytalanságot csökkentsük és ebben az esetben ez sajnos nem történt meg, tehát az információ használhatóságát azzal kell mérnünk, hogy mennyivel járul ahhoz hozzá, hogy a döntéshozatal sikeres lehessen. Minden százalékpontnyi javítás sokba kerül és minél közelebb vagyunk a tökéleteshez, annál több pénzráfordítást igényel.

.

3. Adatvédelem

„A számítógépek megjelenésének kezdetétől az egyik legfontosabb, központi kérdés az adatok és programok biztonsága, védelme. Az első adatvédelmi törvény megjelenésétől (1978) a számítógépvírusok elterjedéséig viszonylag rövid idő telt el, azonban azt láthatjuk, hogy az információtechnológiai szolgáltatások terjedésével, különösen az országokat, földrészeket átszövő hálózatok egyre szélesebb körű alkalmazásával mind nagyobb veszély fenyegeti az adatbázisokat és szoftverrendszereket, tehát az eddiginél is fontosabb a védelemről gondoskodni.” [4]

Ebben a fejezetben az adatvédelemmel fogok foglalkozni. Ismertetem az adatvédelemmel és az adatbiztonsággal kapcsolatos definíciókat, az adatvédelem jogi hátterét, kifejtem azt is, hogy az esetleges emberi vagy természeti vis majorokat hogyan lehet elkerülni vagy az esetleges nem kívánt esemény bekövetkezte után, hogyan lehet a leghamarabb és leginkább költség hatékonyan helyreállítani a szervezet működését.

3.1. Adatvédelem, adatbiztonság és a közöttük lévő különbség

A*datvédelem*nek nevezzük a vállalati adatok gyűjtésének, feldolgozásának és felhasználásának korlátozását, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások adatkezelési eszközök és módszerek összességét. [6] Fontos, hogy a vállalat hálózatában tárolt, nem publikus információkat illetéktelenektől óvjuk, valamint a hálózaton belül lehetővé tegyük, hogy a jogosultak számára az adatok mindig rendelkezésre álljanak.

„Az *adatbiztonság* az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési megoldások rendszere.” [6] Az adatbiztonsággal a következő részben fogok, részletesebben foglalkozni, most csak azt szeretném tisztázni, hogy mi a különbség az adatvédelem és az adatbiztonság között.

Az adatvédelem és az adatbiztonság közötti különbség:

Az adatvédelem (DP- data protection) a vállalaton belül globálisan óvja az információkat, az egész hálózatot védi. Az adatvédelemmel foglalkozó szakemberek próbálják elkerülni, hogy a számítógépekben, hálózatokban sérülések keletkezzenek, az emberi hibákat, a szándékos károkozásokat próbálják kiküszöbölni, megakadályozni. Az adatbiztonság az adatvédelmen belül helyezkedik el, mivel az adatbiztonság is az információk védelmével foglalkozik, de itt a szakemberek már konkrétan az adott dokumentumokat védik a hálózaton belül, hogy illetéktelenek ne férhessenek hozzá, ne módosíthassák, ne olvashassanak bele. Az adatbiztonság a fontos információkat az illetéktelenektől titkosításokkal védi, de eszközei lehetnek a digitális aláírások és egyéb azonosítási eszközök (ujjlenyomat olvasó, chipkártya stb.) egyaránt.

3.2. Vállalaton belül a főbb veszélyforrás

1. *Fizikai veszélyek*
2. *Vállalaton kívüli támadó*
3. *Vállalaton belüli támadó*
4. *Véletlen, nem szándékos károkozás*
5. *Szándékos támadás, alkalmi rosszakaró*
6. *Hardver, szoftver hibák* [11]

Hogyan tudunk e veszélyek ellen védekezni?

1. Fizikai veszélyek alatt a következőkre kell gondolni: tűz, víz, fény, sugárzás, áramkimaradás. „Egy vállalat számítógép parkjának, és a hozzá tartozó környezetnek (hálózat, csatolóelemek, adathordozók) fizikai sebezhetősége fontos tényező a védelem szempontjából. Felmérések szerint a fizikai hibák okozzák a legtöbb üzemzavart, kiesést és kárt, és elhárításuk a legköltségesebb védelmi kiadás. Fontosságához nem fér kétség, hisz a gépek és hálózatok fizikai védelme minden védelem alapját képezi.” [11]

Első és egyik legfontosabb lépés megtervezni, hogy a vállalaton belül hova helyezzük el a számítógépközpontunkat. Lehetőleg ne a legfelső szintre, az esetleges beázások

elkerülése miatt. Ellenőriznünk kell a vízvezetékeket is, hogy ne legyenek a tervezett számítógépterem felett. Ezekkel a lépésekkel minimálisra tudjuk csökkenteni annak a lehetőségét, hogy a víz miatt tönkremenjenek a számítógépek.

Néhány óvintézkedéssel, sok fejtörést megspórolhatunk magunknak. Ilyen óvintézkedés a füstjelző, tűzoltó berendezések elhelyezése az épületen belül, ha véletlenül tűz keletkezne (például egy zárlat miatt), akkor is a lehető leghamarabb hozzá kezdhessünk az oltáshoz, így minimálisra tudjuk csökkenteni a károkat. A tűz kialakulásának valószínűségét csökkenteni tudjuk, ha az épületen belül olyan anyagokat használunk, amelyek kevésbé gyúlékonyak, a tűz terjedését álmennyezet-, padló használatával csökkenthetjük. Másik fontos berendezés a légkondicionáló, amely megakadályozza, hogy a számítógépek túlmelegedjenek, így is csökkenthetjük a meghibásodás veszélyét.

A számítógépek működésük közben mágneses, elektronikus jeleket bocsátanak ki. Ezeket a sugárzásokat megfelelő eszközökkel könnyedén lehallgathatóak és ily módon értékes információkhoz juthatnak a támadók. Az ilyen támadások észrevehetetlenek, mivel a számítógép tartalmához nem nyúlnak. A kívülről jövő sugárzásokkal, pedig bizonyos számítógépes eszközöket tehetnek tönkre, ilyen eszközök például mágnesszalag, floppy. A sugárzást meglehet szüntetni, ha különféle fémből készült árnyékoló eszközöket alkalmazunk.

Az áramkimaradások ellen szünetmentes tápegységekkel vagy generátorral védekezhetünk, így elkerülhetjük az adatvesztést és az informatikai eszközeink rongálódását is a hirtelen áramkimaradás miatt.

2. *Vállalaton kívüli támadók*, lehetnek a betörők. A vállalat értékeit riasztó felszerelésével védhetjük meg a külső behatolóktól.

3. *Vállalaton belüli támadók,* lehetnek az ott dolgozók. Általában az adatokkal való visszaélésre adhat okot, a bosszúvágy, a vagyonszerzés, az irigység, de itt a gondatlanság, nemtörődömség is előfordulhat, ezért a védekezésnél nagy figyelmet kell a felhasználókra fordítani. A vállalaton belüli dolgozók ellen többféleképpen védhetjük az értékeket. Ilyen megoldás lehet, ha mindig zárjuk azt a termet, ahol a számítógépeket tartjuk, ezt különböző beléptető berendezéssel vagy kulcs használatával is elérhetjük, így csak azok az emberek férhetnek majd a gépekhez, akik az adott teremben dolgoznak is. Fontos, hogy a hozzáférési jogokat korlátozzuk. A vállalaton belüli dolgozók, csak a feltétlenül szükséges jogokat kapják meg, ezzel is csökkenthető a visszaélések száma. Lehetőség szerint minden számítógépet csak

egy ember használjon, de ha ez nem megoldható, akkor alkalmazzunk több szintű jelszavas védelmet vagy többfaktoros védelmet (különböző védelmi eszközök kombinációja).

4. Véletlen, nem szándékos károkozás: törlés, módosítás. Általában ezek a károkozások gondatlanságból, tudatlanságból történnek meg. A véletlen törlések és módosítások ellen, biztonsági mentésekkel védekezhetünk. Minden fontos információt három példányban, különböző időpontokban (generációs mentés) mentsünk. A különböző mentéseket egymástól fizikailag elkülönített helyeken tároljuk, az esetleges rongálódás (például tűz) elkerülése miatt. Erre megfelelő lehet adatbázis bérlése.

Mentési típusok: A mentés alatt a tárolt információ biztonsági másolatát vagy másolatok készítését értjük. A még használatban lévő adatokról is kell készíteni másolatot, hiszen az elveszett, sérült adatokat vissza tudjuk állítani.

- *Teljes mentés*: Az összes adatot menti a számítógépeken. Rendszeres időközönként végzik. (kb. hetente)
- *Különbözeti mentés*: Csak az utolsó mentés óta bekövetkezett változtatásokat menti a számítógép. Naponta ajánlott elvégezni.
- *Részleges mentés*: Előre meghatározott adat, adatcsoportok teljes mentése.
- *Null mentés*: a rendszer induló állapotát mentjük. [11]

5. Szándékos támadás, alkalmi rosszakaró: számítógépvírusok. A számítógépvírusok ellen, úgy tudunk védekezni, ha a rendszertől elzárjuk a jogosulatlan felhasználókat és jogtiszta szoftvereket használunk. Soha ne nyissunk meg gyanús, ismeretlen fájlokat. A levelezőprogramok biztonsági szűrőit használjuk. Alkalmazzunk, olyan víruskereső szoftvert, amely rendszeresen frissíti magát a legújabb vírusdefiníciókkal, így mindig naprakészen védhetjük rendszerünket a kártékony behatolókkal szemben. A vállalati hálózatokon belül webszűrők alkalmazása ajánlott, ahol a veszélyes honlapokat a felhasználók számára elérhetetlenné tesszük. Ajánlott a vállalaton belül, belső hálózatot kialakítani. Az ilyen belső hálózatot Intranetnek nevezzük, amely az Internet-protokollt használja, de a külvilág, az illetéktelen behatolók előtt zárt. Tűzfallal védik ezeket a hálózatokat. Általában egy-egy vállalaton belül alkalmazzák. A vállalaton belül minden dolgozó személyre szabott jogosultságokat kaphat, hogy ne férhessenek hozzá minden adathoz a hálózaton belül, ezzel is csökkentik a kockázatot, hogy visszaélhetnek a dolgozók a vállat adataival.

6. Hardver, szoftver hibák. A hardverhibákat tükrözéssel védhetjük ki. A szoftverhibákat elkerülhetjük, ha megbízható, jó minőségű, jogtiszta szoftvereket alkalmazunk és egységes szoftver csomagokat alkalmazunk, így a szoftverek összehangoltságából eredő hibákat elkerülhetjük.

A most felsorolt 6 vállalaton belüli fő veszélyforrást a következő táblázatban összefoglalva is megtekinthetjük:

<table>
<tr><th colspan="5">Adatvédelem</th></tr>
<tr><th colspan="2">Az emberek adatainak védelme</th><th colspan="3">Az adatok védelme</th></tr>
<tr><td>Az egyéni adatok Titkossága</td><td>Az információrendszer egyensúlyának megzavarása</td><td>Tűz, víz, fény, mágnesezési hatásoktól, betöréstől, lopástól</td><td>Adatgyűjtési, tárolási, átviteli, feldolgozási hibáktól</td><td>A dolgozók, a kalózok és a vírusok okozta károktól</td></tr>
<tr><th colspan="5">A megvalósítás módja</th></tr>
<tr><td colspan="2">Az adatvédelmi törvény megalkotásával és betartatásával. Az adatok tárolása csak a törvényi előírások és az egyének akaratával lehetséges.</td><td>Többgenerációs mentésekkel</td><td>Ellenőrző kódok alkalmazásával, ellenőrzési érvényességi vizsgálatokkal</td><td>Elzárással, ellenőrzéssel, hozzáférési jogok korlátozásával.</td></tr>
</table>

1. táblázat: Adatvédelem [4]

3.3. Adatvédelem jogi szabályozása Magyarországon

Az adatvédelem jogi szabályozása akkor vált fontossá, amikor az Internetnek köszönhetően a távoli hálózatok összekapcsolódtak egymással és így megkönnyítették, hogy a különböző adatokat társíthassák egymással (összehasonlítás, elemzés stb.). Sokkal egyszerűbbé vált a különböző személyes adatokhoz, üzleti titokhoz hozzá férni, ezért elkerülhetetlenné vált, hogy törvényes keretek között szabályozzák, ki, milyen adatokat és milyen módon kezelhet, használhat fel. Az adatvédelmet érintő törvények tükrözik egy ország demokratikus berendezésének fokát. Magyarország adatvédelmi törvényei megfelelnek

az Európai Uniós szintnek. Folyamatosan egészítik, pontosítják a már meglévő törvényeket, a különböző adatbiztonsági fejlődések hatására.

3.3.1. Az adatok fajtái

1. *Személyes adat*: Minden olyan információt személyes adatnak nevezünk, aminek a segítségével bármely természetes személy azonosítható vagy kapcsolatba hozható. Az adatokat személyes jellegűnek, addig tekintjük ameddig az adott egyén személyisége kikövetkeztethető belőle. A személyt azonosítani lehet, neve, lakcíme, személyi azonosítója, stb. alapján.
2. *Különleges adat:* A jogvédelem azon alapszik, hogy a magánéletben leginkább védelemre szoruló adat, illetve az illetéktelen hozzáférés a legnagyobb sérelmeket okozhatják az egyén számára. [1] Ilyen különleges adat: a faji eredetre, a nemzeti és etnikai hova tartozásra, a politikai pártállásra, a vallásos vagy más világnézeti meggyőződésre, az egészségi állapotra, a káros szenvedélyre, a szexuális életre, valamint a büntetett előéletre vonatkozó személyes adat.
3. *Közérdekű adat**:*** az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, a személyes adat fogalma alá nem tartozó adat. [2]

3.3.2. Törvények

[2]

<u>1992. évi LXIII. Tv.:</u>

A Magyar Országgyűlés 1992. őszén fogadta el és 1993. május 1-én lépett hatályba, az első adatvédelemmel kapcsolatos törvényt, amely a személyes adatok védelméről és közérdekű adatok nyilvánosságra hozataláról szólt. A hazai adatvédelmi szabályozás

legjelentősebb törvénye, mivel ebben írták le az alapvető adatvédelmi törekvéseket, a későbbi törvények csak ennek a törvénynek a kiegészítésének felelnek meg.

A törvényben a személyes és közérdekű adatokat külön tárgyalja, de mivel az egyik a másiktól elválaszthatatlan, ennek hatására egy törvénybe foglalták. Nem tesz különbséget számítógépes vagy írásos adatállomány között.

Célja, hogy a személyes adataikkal mindenki maga rendelkezhessen és a közérdekű adatokat mindenki megismerhesse.

A törvény a következőket tartalmazza:

-*Adatkezelés:* A személyes adatok felvétele és tárolása, feldolgozása, hasznosítását, módosítása vagy a további felhasználása az adatkezelés feladatkörébe tartozik.

-*Adattovábbítás:* ha a személyes adatokat 3. fél számára hozzáférhetővé tesszük akkor adattovábbítást végzünk.

-*Adatkezelő:* az a természetes vagy jogi személy illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely a személyes adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.

-*Adatfeldolgozó:* Az adatkezelő megbízásából személyes adatok feldolgozását végzi.

-*Adatkezelés:* Személyes adatokat csak akkor kezelhetnek, ha az érintett személy hozzájárul, vagy törvény által előírják. Személyes adatokat előre meghatározott céllal lehet csak kezelni és csak a cél megvalósításához elengedhetetlen személyes adat kezelhető. Az érintettel közölni kell, hogy az adatszolgáltatás önkéntes vagy kötelező. Tájékoztatni kell az adatkezelés céljáról és arról hogy kik kezelik az adatokat.

-*Nyilvánosságra hozatal:* A személyes adatokat csak akkor szabad nyilvánosságra hozni, ha az a közérdekében történik vagy az érintett ehhez írásban hozzájárul.

-*Adatvédelmi biztos:* Biztost azért választanak, hogy a személyes adatok védelméhez és a közérdekű adatok nyilvánosságra hozatalához való alkotmányos jogokat védje.

Feladata: -Kivizsgálja a hozzá beérkező bejelentéseket,

-Ellenőrzi a törvények betartását,

-Gondoskodik az adatvédelmi nyilvántartás vezetéséről.

1992. évi LXVI. Tv.**:**

Az állampolgárok személyi adatainak és lakcímének nyilvántartásáról szól:

E törvény alapján a hatóságok kötelesek személyes és lakcím adatainkat nyilvántartani és ezeket frissíteni adatváltozások esetén. Minden Magyarországon élő személyre vonatkozik, így a bevándoroltakra, a hazánkban letelepedettekre, valamint a menekültként elismert személyekre is egyaránt.

1995. évi LXV. Tv.:

Az államtitokról és a szolgálati titokról szóló törvény**:**

Államtitok: Sérti vagy veszélyezteti a Magyar Köztársaság honvédelmi, nemzetbiztonsági, bűnüldözési vagy bűnmegelőzési, központi pénzügyi vagy devizapolitikai, külügyi vagy nemzetközi kapcsolataival összefüggő valamint igazságszolgáltatási érdekeit.

Szolgálati titok: Sérti az állami vagy közfeladatot ellátó szerv működésének rendjét, akadályozza a feladat- és hatáskörének illetéktelen befolyástól mentes gyakorlását.

1996. évi XX. TV.:

A személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szól. Rendelkezik az adóazonosító jel és a TAJ számáról. Pontosan leírja, hogy a különböző személyazonosítókat hol és milyen körülmények között alkalmazhatják. A személyazonosító jel személyes adatnak minősül, ezért korlátozzák a hozzáférési jogokat. Ez sok szervezet számára megnehezítette a különböző adatbázisok létrehozását, mert eddig a különböző személyeket ezek alapján egyszerűen azonosíthatták.

1996. évi CXII. TV.:

Banktitokkal a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény:

Banktitok: Az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló, tény, információ, megoldási mód vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik.

Harmadik félnek akkor adható ki, ha:

-pénzügyi intézmény ügyfele a rá vonatkozó adatokat hivatalosan kéri

-ha a törvény felmentést ad
-ha a pénzügyi intézmény érdeke ezt az ügyféllel szemben fennálló követelése eladásához vagy lejárt követelése érvényesítéséhez szükségessé teszi.

3.4. Kockázatmenedzsment

3.4.1. Kockázatelemzés

A vállalatok életében fontos, hogy minden egyes negatív hatással szemben megfelelően felkészültek legyünk. Minden eshetőséggel számolni kell, mivel nem mondhatjuk azt később, hogy ennek az eseménynek a bekövetkeztére nagyon kicsi volt az esély és ezért nem is számoltunk vele. A kockázatmenedzsment a kockázatok elemzésével és kezelésével foglalkozik.

Az Egyesült Királyságban a kockázatelemzésre The Central Computer and Telecommunications Agency *(*CCTA*)* kifejlesztett egy módszertant, a CRAMM-ot (CCTA Risk Analysis Managment Method), amely sorba veszi egy vállalat lehetséges sebezhető pontjait, a ráleselkedő veszélyeket és ajánlást tesz az esetleges megelőzésre.

3.4.1.1. A kockázatelemzés főbb részei a következők
[14]

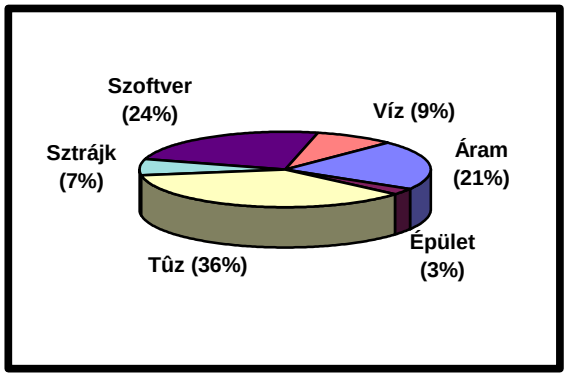
1. *A vállalat eszközeinek sorba vétele és értékelése:* A vállalat információ-technológiai eszközeit és adatait egyesével sorba veszik és értékelik, hogy mennyire sérülékenyek és milyen veszélyeknek vannak kitéve.
2. *A fenyegetések felbecslése:* A informatikai rendszerek szándékos vagy véletlen rongálódásának bekövetkeztének valószínűségét állapítjuk meg a kockázatelemzésnek ebben a szakaszában.

Egy vállalatra leselkedő veszélyforrások a következők lehetnek:

- a tűz, víz vagy természeti csapás által okozott károk,

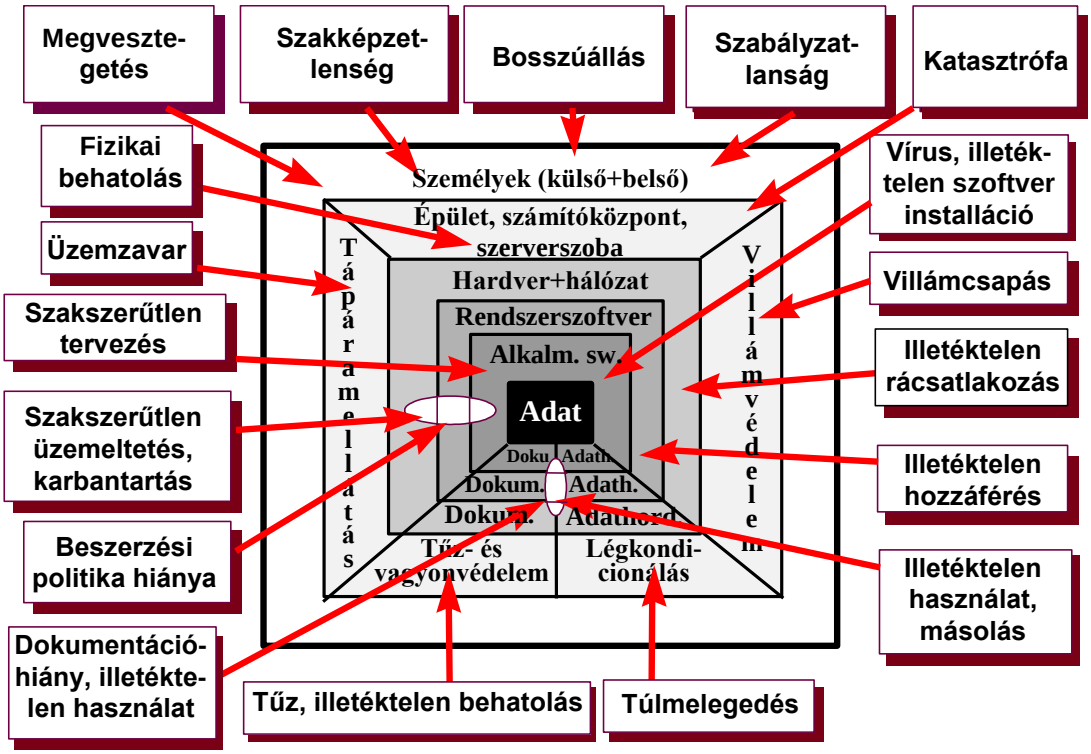
- tudatos rombolás és eltulajdonítás,
- rendszer szoftver, hardver, áram vagy egyéb környezeti kiesés. [8]

Ezeknek az eseményeknek, a bekövetkeztének valószínűségét mutatja a következő ábra.



3. ábra: A katasztrófák okainak aránya

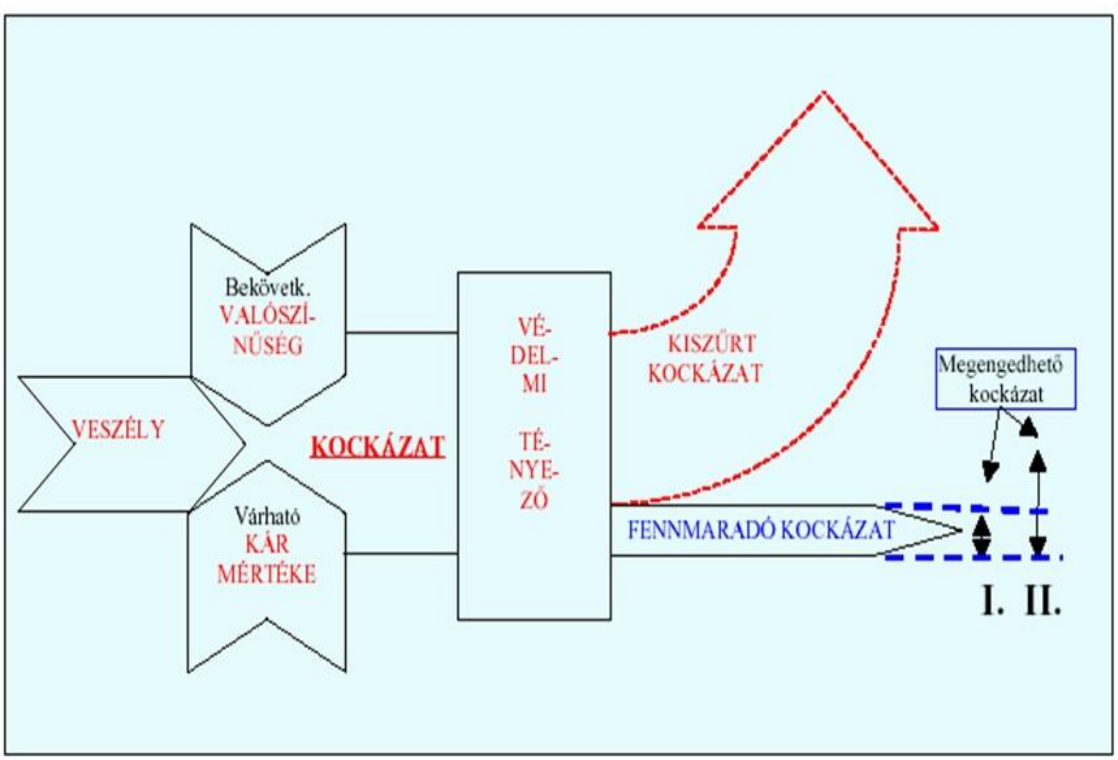
Az előző ábrán látott események részletesebb felbontását láthatjuk a 4. ábrán, ahol a szervezet egyes részeire leselkedő fenyegetettségeket nézhetjük meg:



4. ábra: Egy szervezetet érintő fenyegetettségek

3. *A sebezhetőség felbecslése*: Sorba vesszük, hogy az 1. pontban meghatározott vállalati eszközökre, milyen mértékű veszélyeket jelent a 2. pontban felsorolt fenyegetettségek.
4. *Kockázatbecslés:* Ebben a pontban mérlegeljük, a különböző eszközök megsérülésének a valószínűségét, a sérülésekre való érzékenységét, valamint az eszközök értékét vizsgáljuk. A *kockázat*ot a gyakoriság és a súlyosság szorzataként számíthatjuk ki.
5. *Ellenintézkedések kiválasztása:* A megfelelő biztonsági ellenintézkedéseket választjuk ki, amelyek költség hatékonyan képesek, a kockázatot elfogadható szintre csökkenteni**.**

Az 5. ábra a kockázatelemzés feladatkörét összegzi:



5. ábra: Kockázatelemzés folyamata

Fontos megjegyezni, hogy a vállalat információ-technológiai eszközeinek biztonsági szintjét a leggyengébb pontja határozza meg, mivel egy esetleges rosszakaró a vállalatnak azt a pontját fogja támadni, ahol legkönnyebben sebezhető, ezért ezeknek a pontoknak a védelmére kell a legtöbb energiát fordítani.

3.4.2. Katasztrófa-elhárítás

[3]

A kockázatmenedzsment a kockázatelemzés mellett, a katasztrófa elhárításával is foglalkozik. Fontos, hogy egy vállalat rendelkezzen katasztrófa-elhárítási tervvel, mivel így elkerülhető, hogy egy esetleges fenyegetettség bekövetkeztekor a vállalat működése hosszabb időre felboruljon, leálljon. A katasztrófa-elhárítási tervnek részletesnek és pontosnak kell lennie. A terv elkészítése során, minden információ-technológiai elemre figyelni kell, mivel bármelyik elem figyelmen kívül hagyása esetén aláásható az egész terv használhatóságát. A vállalat dolgozóinak, bármilyen esemény bekövetkeztekor tisztában kell lenniük azzal, hogy kinek mi a feladata és milyen teendőket kell elvégezni az adott szituációban. Például, ha egy vállalat számítógép központját egy csőtörés következtében elárasztotta a víz, és így az informatikai rendszere használhatatlanná vált, akkor se engedheti meg magának a vállat, hogy napokig vagy hetekig zárva legyenek, mert az ügyfelek más vállalatokhoz mennek a problémájukkal, így hamar csődbe mehetnek. Ha van egy jó katasztrófa elhárítási tervük, akkor akár órákon belül helyre állhat a rend és folytatódhat a munka, mintha mi sem történt volna.

A szervezetek informatikai függősége folyamatosan nő, fontos, hogy szolgáltatásaikat megfelelő minőségben és időben nyújtsák. Mivel ha nem állnak rendelkezésre az adott szolgáltatások, akkor a szervezethez forduló felhasználó, nem tudja napi teendőit elvégezni és ezért másik céghez fog fordulni.

Katasztrófa-elhárítási tervre azért van szükség, hogy a következő lehetséges következményeket elkerüljük:

- Információvesztés
- A kommunikáció megszakadása

- A biztonság megsérülése
- A kritikus alkalmazások leállása
- Az ügyfelek megbecsülésének elvesztése
- Az alapvető tevékenységek megszakadása [8]

A katasztrófa-elhárítás tervezése:

A katasztrófa-elhárítási tervben nem csak az informatikai eszközök és hozzájuk kapcsolódó berendezések védelmére kell gondolni, ilyenkor az egész szervezetre kell figyelmet fordítani, ilyen egyéb eszközök lehetnek például a papíralapú információk, amelyek természetesnek tűnnek, hogy a szervezet alkalmazásában állnak, de a védelmére általában nem gondolnak.

A katasztrófa-elhárítás tervezése nagyon sok időt, energiát és pénzt igényel és a szervezeti vezetőknek nehezen látható át, hogy tulajdonképpen mit is kapnak, ezen erőfeszítések után cserébe.

A katasztrófákat minden esetben először meg kell próbálni megelőzni, ezeket a szükséges lépéseket az adatvédelem résznél tárgyaltam. Itt csak újra felsorolom, emlékeztetőképpen:

- beléptető rendszerek,
- tűzjelző és tűzoltó berendezések,
- adat és szoftver védelmi eljárások,
- karbantartó eljárások.

A katasztrófa-elhárítás tervezésének lépései:

1. A kockázatelemzés értékelésével kezdjük, ezután minden egyes szolgáltatás kiesésének hatását értékeljük. Mennyire nagy kárt okozhat az adott rész átmeneti hiánya.
2. A szolgáltatások, vállalati részlegek közül meg kell határozni, hogy melyek azok, amelyekre feltétlenül szükség van és üzemelniük kell. Ezekre a területekre kell a legnagyobb figyelmet fordítani és gondoskodni kell a lehető leghamarabbi üzemképességéről.

3. Fontos meghatározni azt az időintervallumot, amely alatt a szolgáltatásoknak újra működőképesnek kell lenniük:
   - n órán belül,
   -n napon belül,
   -nem kritikus.
4. Az informatikai és egyéb eszközök helyreállításához szükséges eszközök meghatározása.
5. A katasztrófa-elhárítási terv alapváltozatai közül kiválasztani a megfelelőt:

Katasztrófa-elhárítási alapváltozatok

A vállalatok vezetői, ezekből az alapváltozatokból választják ki azt, amelyik leginkább megfelel a szervezet számára, a katasztrófa-elhárítási terv készítésére.

1. *Semmit sem teszünk:* Ennek az alapváltozatnak az a veszélye, hogy bármelyik, a vállalatot veszélyeztető katasztrófa bekövetkezhet. Az IT eszközök védelmének érdekében ez a lehető legrosszabb döntés. Ha a számítástechnikai eszközökön lévő információk nem fontosak annyira, hogy a védelmére pénzt áldozzanak, akkor miért használ az adott vállalat informatikai eszközöket?
2. *Kézi helyettesítő eljárásokat alakítunk ki:* Napjainkban már elég nehéz a számítógépeket manuálisan helyettesíteni, mivel sokkal gyorsabban és pontosabban dolgoznak, mint az egyén. Nem is kifizetődő, mivel sokkal több emberre van szüksége egy vállalatnak, ha informatikai eszközök nélkül próbálja megoldani a helyettesítést.
3. *Kölcsönösségi egyezményt kötünk:* Itt két kompatibilis szervezet egyezséget köt egymással, hogy szükség esetén a másik szervezet informatikai eszközeivel pótolja saját kieső szolgáltatásait. A gyakorlatban ez a megoldás nem túl népszerű, mivel félő hogy a másik szervezet saját szolgáltatásainak rovására megy, ezeknek a tesztelése is jelentős problémákat okozhatnak.
4. *"Erőd" megközelítés:* Az 1. alapváltozat ellentétjének felel meg. A lehetséges fenyegetettségek bekövetkeztének valószínűségét a minimálisra próbálja csökkenteni, annak érdekében, hogy az IT szolgáltatásait folyamatosan működtetni

tudja. Ebben a változatban esetleges második telephelyről nem gondoskodik, inkább a központi telephely biztonsági eszközeire költ komoly összegeket.

5. *"Hideg" indítású fix megközelítés:* Egy üres számítógép termet bérel a szervezet, ahol megvannak a szükséges feltételek, hogy egy vállalati hálózat működni tudjon. Az informatikai eszközöket a vállalatnak saját magának kell biztosítania.
6. *"Hideg" indítású szállítható megközelítés:* Ebben az esetben is a vállalatnak kell biztosítania a megfelelő informatikai eszközöket. Itt a termet szállítják arra a helyre, ahol a vállalat az ideiglenes informatikai hálózatát szeretné felállítani. A terem itt is rendelkezik a hálózat működéséhez szükséges feltételekkel.
7. *"Meleg" indítású külső megközelítés:* Nagy-Britanniában már léteznek olyan szervezetek, amelyek olyan telephelyet és informatikai eszközöket biztosítanak, ami a szolgáltatást, igénybevevő elvárásait teljes egészében kielégíti. Ennek a költségei attól függenek, hogy milyen szintű informatikai eszközökre van szüksége az adott szervezetnek (például: szoftver és hardver típus, számítógépek száma). Az ilyen szolgáltatást nyújtó szervek általában korlátozott ideig nyújtják szolgáltatásait, mivel több előfizetője is van.
8. *"Meleg" indítású belső megközelítés:* A vállalat saját magának biztosít egy telephelyet a megfelelő információ-technológiai eszközökkel együtt. Ha nincs vészhelyzet, akkor ezt a telephelyet akár fejlesztésekre vagy különböző tesztelésre is lehet használni, ha pedig valamelyik fenyegetettség bekövetkezik, akkor ideiglenesen a fejlesztéseket, teszteléseket fel lehet függeszteni és így zavartalanul működhet tovább a szervezet.
9. *"Meleg" indítású szállítható megközelítés:* Egy szolgáltató biztosítja a szükséges IT szolgáltatásokat és ezt egy szállítható teremben, olyan helyen helyezi el, ahova a szolgáltatást igénybevevő kéri. Ez a *"Hideg" indítású szállítható megközelítés* és a *"Meleg" indítású külső megközelítés* kombinációja.

A katasztrófa-elhárításnak köszönhetően, rávilágíthatunk a vállalat gyengepontjaira és ezzel megtudhatjuk, hogy mely részlegekre kell nagyobb figyelmet fordítani. A terv arra is világosan kitér, hogy pontosan mikor és hogyan kell alkalmazni a leírtakat. Pontos útmutatást ad, hogy a vállalaton belül ki felügyeli a helyreállítási munkálatokat az egyes katasztrófák esetén.

Katasztrófa-elhárítási terv előnyei:

- Elsődleges célja, minimálisra csökkenteni a különböző katasztrófák bekövetkeztének valószínűségét, vagyis a kockázati szintet minimalizáljuk.
- A tervvel csökkentjük a kiesési időt, így a szolgáltatások folytonos elérési ideje növekszik a felhasználók számára.
- A vállalat számára minimálisra csökkentjük a megszakítási időt.
- A költségek szempontjából a leghatékonyabb katasztrófa-elhárítási megoldást tudjuk választani.

4. Adatbiztonság

Az adatbiztonság annak köszönheti kialakulását, hogy az emberek igényt tartottak arra, hogy egymástól távol élő személyek bizalmas üzenteteket válthassanak egymással. Az ókori görögök már kr.e. 404-ben alkalmazták a perzsák várható támadásával kapcsolatban az adatbiztonság eszközeit, az úgynevezett szkütalé szalagot, amely egy sokszögalakú hasábra vagy pálcára felcsavart szalag volt. A szalagra felírták a rejtjelezni kívánt szöveget, a pálca tengelyének irányában, ezután letekerték a szalagot és addig olvashatatlanná vált, ameddig egy ugyanolyan alakú pálcára vissza nem tekerték.

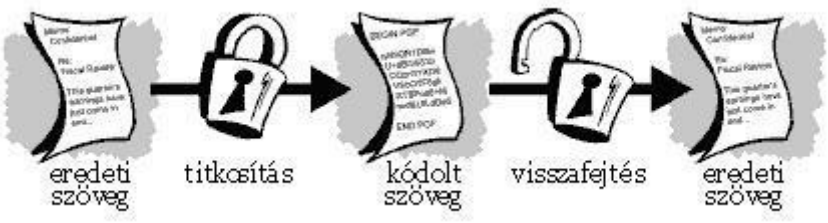
Az *adatbiztonság* az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési megoldásokkal foglalkozó tudomány. [11] Fontos, hogy adatainkat védjük a rosszindulatú felhasználók ellen. Az adatvédelem kisebb szegletébe tartozik az adatbiztonság. Az adatvédelem, ahogy az előző fejezetben is láthattuk, globálisan védi az információkat a jogosulatlan hozzáférőktől, míg az adatbiztonság ennél szűkebben védelmezi azokat.

Miért fontos az adatbiztonság?

Az emberek mindennapi életében természetessé vált a számítógép és az Internet használata. Ezeknek az eszközöknek köszönhetően, világméretű hálózatok jöttek létre, ahol már szinte bármilyen adat elérhetővé vált az ember számára, ezért a személyes és érzékeny adatokat védeni kell, hogy ne kerüljenek illetéktelen kezekbe és ne tudjanak ezekkel visszaélni, ellenünk fordítani. Legegyszerűbben titkosítással, rejtjelezéssel tudunk védekezni ezeken a hálózatokon.

4.1. Titkosítás

A következő ábra a titkosítás (kriptográfia) általános alakját mutatja be:



6.ábra: Titkosítás folyamata

A titkosítás folyamata:

A feladó egy fontos dokumentumot szeretne eljuttatni tikosítva egy másik félnek (a Címzettnek). A feladó titkosítja a dokumentumot egy titkos kulccsal, majd ezt a dokumentumot valamilyen csatornán keresztül eljuttatja a címzettnek. A címzettnek, pedig vissza kell fejtenie a kódolt dokumentumot. A címzett kétféle kulccsal dekódolhatja az üzenetet, attól függően, hogy a feladó milyen titkosítást alkalmazott:

1. Szimmetrikus titkosítással (egykulcsos): Ebben az esetben a címzett ugyanazt a kulcsot használja, amelyiket a feladó is használta, mivel a titkosító és a visszafejtő, dekódoló kulcsok megegyeznek vagy egyikből a másik kulcs könnyedén kiszámítható. Ekkor a feladónak és a címzettnek találkozniuk kell, hogy a kulcscserét elvégezhessék vagy vállalniuk kell annak kockázatát, hogy a hálózaton keresztül, ahol a csere megtörténik, harmadik fél is hozzájuthat. A titkosító és a visszafejtő kulcsokat titokban kell tartani. Ennek a titkosításnak nagy előnye, hogy gyors és nagy dokumentumok titkosításánál is alkalmazhatjuk. Hátránya viszont, hogy mindegyik féllel, akikkel kommunikációt folytatunk más és más kulcsot kell használnunk, mivel ha egy kulcsot használnánk akkor egymás üzeneteit is eltudnák olvasni.

2. Aszimmetrikus titkosítással (kétkulcsos): Ebben az esetben a címzett már egy másik kulcsot használ dekódolásra, mivel ennél a titkosításnál egy kulcspárt alkalmazunk (egy nyilvános és egy titkos kulcsot). A nyilvános kulcs terjeszthető, míg a másik kulcsot titokban kell tartani. A titkosító és a dekódoló kulcsok olyannyira különböznek, hogy egyik kulcsból se tudjuk a másik kulcsot meghatározni. A címzett nyilvános kulccsal tudja a feladó titkosítani az üzenetet, ezt az üzenetet csak a címzett (a titkos kulcs tulajdonosa) tudja visszafejte. Itt a személyes kulcscsere nem szükséges. Ez a titkosítási módszer lassabb, ezért kisebb dokumentumok kódolásánál alkalmazzák.

4.2. Támadások

A támadásokat megkülönböztethetjük attól függően, hogy a támadók az üzenetet módosítják vagy sem. A támadó célja minden esetben az, hogy a titkosított üzenet tartalmát megszerezze.

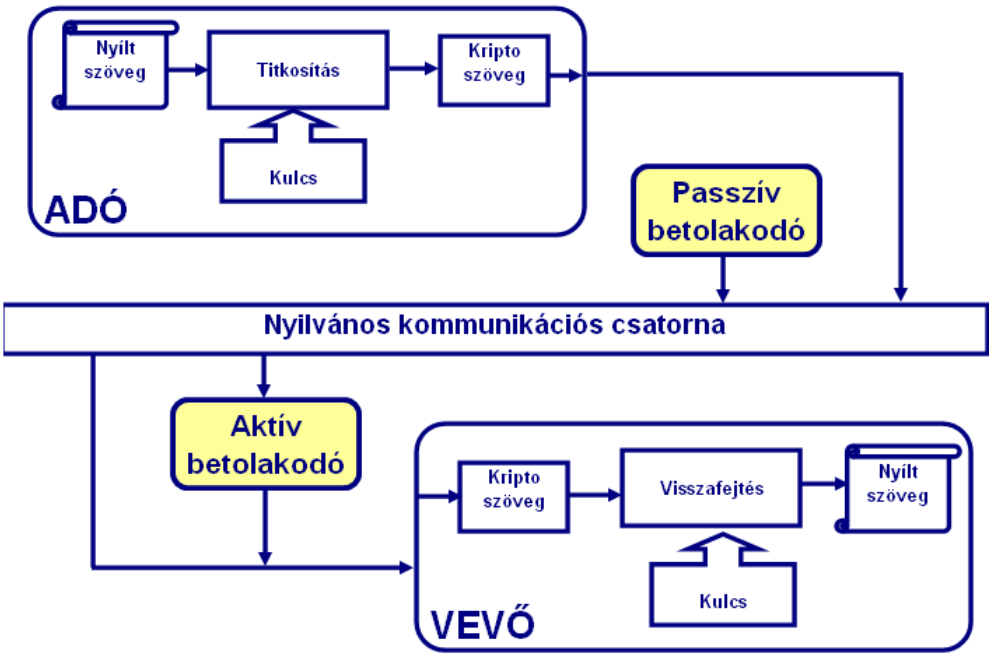
Passzív támadásról akkor beszélünk, ha a támadó csak megfigyelőként van jelen, a titkosított üzeneteket lehallgatja, esetleg archiválja, de a meglévő információkon módosításokat nem hajt végre. Passzív támadásra példa, a rendszer elemeinek elektromágneses kisugárzásán alapuló lehallgatása, itt a hálózattal közvetlen kapcsolatban sem kell lennie a támadónak, ezért ezt a támadást nagyon nehéz észlelni.

Aktív támadásról akkor beszélünk, ha a támadó nem csak megszerzi a titkos információt, hanem módosítja is azt. Ezt többféleképpen tudja megtenni:

-Az üzenetet módosítja, oly módon hogy az a támadó számára kedvező legyen.

-Megszemélyesítés, esetén a támadó beépül a kommunikációs csatornába, így az üzenetekhez hozzáfér, és a kommunikációban résztvevő másik fél helyett válaszol, mindkét irányba.

A ábrán láthatjuk ezeket a támadási formákat.



7. ábra: Aktív, passzív támadás

4.3. Partner-azonosítás

Célja az egyed identitásának bizonyítása. Az adatbiztonság fontos részét képezi, mivel a partner-azonosítás segítségével ellenőrizhetjük a vállalaton belül, hogy ki jogosult az információk hozzáféréséhez.

4.3.1. Fajtái

1. *Biometrikus* (újlenyomat, retinavizsgálat, szemírisz vizsgálat, hanganalízis),
2. *Birtok alapú* (beléptető kártya),
3. *Tudás alapú* (jelszó).

1. *Biometrikus**:*** ” Egy olyan automatikus technika, amely méri és rögzíti egy személy egyedi fizikai, testi jellemzőit és ezeket az adatokat azonosításra és hitelesítésre használja fel. A biometrikus felismerés alkalmazható személyazonosítás céljára, amikor a biometrikus rendszer azonosítja a személyt, az egész lajstromozott adatállományból kikeresve a megegyezőt. A rendszer használható továbbá ellenőrzési célból, amikor a biometrikus rendszer hitelesít egy személyt az előzőleg bejegyzett mintái alapján. Egy sor különleges előnyt kínál a biometria alkalmazása személyazonosság- és jogosultságvizsgálat céljára. Csak a biometrikus azonosítás alapul ugyanis az emberek valódi, tőlük elválaszthatatlan azonosságán.„ [12] A biometrikus technikák alkalmazása azért célszerű, mert ezekkel a rendszerekkel lehet a legnehezebben visszaélni. A beléptető kártyákat elhagyhatjuk, a jelszavakat megfejthetik vagy azok a felhasználók, akik a biztonságot nem veszik komolyan akár el is árulhatják másoknak a jelszavaikat. Az ujjlenyomatunk, íriszünk, hangunk mindig velünk van, nem tudjuk elhagyni és más embereknek se tudjuk átruházni.

A biometrikus azonosítók közül napjainkban az *ujjlenyomat-azonosítás* a legelterjedtebb: Az ujjlenyomat minden egyednél különböző, ezért minden felhasználót pontosan lehet vele azonosítani. A ujjlenyomat olvasó, meghatározott számú pontot rögzít és ezen adatok alapján, gyorsan és könnyedén vissza tudja keresni az adatbázisban a lenyomathoz tartozó személyt. A

felvett mintából a lenyomatot rekonstruálni nem lehet, így személyiség jogokat se sért. Ujjlenyomat azonosítót alkalmaznak például a rendőrségen, ahol az ujjlenyomat-olvasó segítségével az adatbázisában lévő büntetett előéletű embereket, hamar vissza tudják keresni egy esetleges újabb bűntény kapcsán.

2. *Birtok alapú:* Partner-azonosítási eszköz, valamilyen fizikai eszköz birtoklása. Például: beléptető kártya. Ezeknek a működési elve a biometrikus partner-azonosítási elven működik, csak itt nem az egyed különböző testrészeit vizsgálja, hanem a beléptető kártyáját, ez is minden dolgozó számára más, ezért ennek segítségével akár a dolgozók munkaidejét is vizsgálhatjuk.
3. *Tudás alapú:* Valamilyen titok ismeretén alapszik. Például egy jelszó vagy digitális kulcs ismerete.

Jelszó: Napjainkban a leggyakrabban alkalmazott partner-azonosítási eszköz, mivel használata egyszerű, olcsó, könnyen kivitelezhető és odafigyeléssel biztosítani tudja a megfelelő védelmet.

A jelszó használatát biztonságosabbá tehetjük, ha néhány egyszerű szabályt alkalmazunk:

-Ha a támadó találgatásos módszerrel próbálja a jelszavunkat feltörni, nagy valószínűséggel, a személyünkkel kapcsolatos adatokkal próbálkozik (például: születési dátum, kiskutyánk neve stb.), ezért ezeket kerüljük.

-Egyszerű, könnyen kitalálható szótári szavak alkalmazása se ajánlott, mivel ezek is könnyen megfejthetőek, szótár alapú támadásokkal. Helyette olyan karaktersorozatot alkalmazunk, amely kis- és nagybetűk mellett számokat és különleges karaktereket is tartalmaz.

- A jelszavakat gyakran cseréljük, így is csökkenthetjük a támadás valószínűségét.

- Minden felhasználói felületen más és más jelszót használjunk

- Érdemes maximális hosszúságú jelszót választani, ez is javítja a rendszer biztonságát. A következő táblázatban látható, hogy a különböző karakterek használata mellett mennyi időbe telik egy 6 illetve 8 betűs jelszó megfejtése:

Karakterkészlet	Jelszó hossza	10000 jelszó/sec	1000000 jelszó/sec
(a - z)	6	8.58 óra	5.15 perc
	8	241.7 nap	58.1 óra
(a – z, 0 – 9)	6	2.52 nap	36.28 perc
	8	8.94 év	32.65 nap
(A – Z, a – z)	6	22.8 nap	5.49 óra
	8	169.41 év	1.69 év
(A – z, 0 - 9)	6	65.74 nap	15.78 óra
	8	691.9 év	6.92 év

2. táblázat: Az egyes jelszavak feltörésének ideje [11]

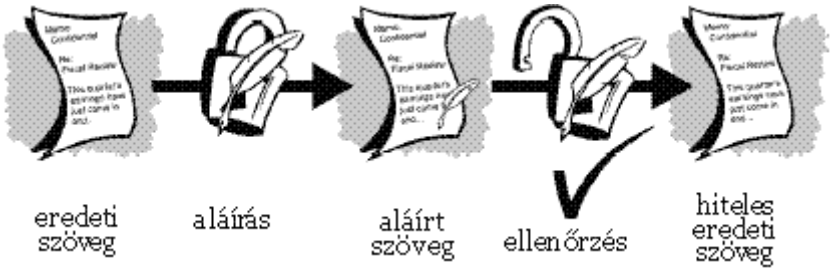
4.4. Digitális aláírás

Az Internetnek köszönhetően megszűnt az idő és térbeli korlát. Ma már lehetőségünk van arra, hogy a világ más pontján lévő partnerrel üzletet kössünk úgy, hogy bármelyiküknek is több száz vagy ezer kilométert kellene utazni, de hivatalos ügyeinket is intézhetjük az Interneten keresztül, ehhez azonban szükségünk van arra, hogy hitelesen azonosítani tudjuk magukat, ezt digitális aláírással megtehetjük.

A *digitális aláírás* segítségével meggyőződhet arról a címzett, hogy a neki küldött üzenetet, a levél küldése során nem módosították és a feladó tényleg az, akinek mondja magát. A digitális aláírással a felek számára bizonyítható, az adatállomány eredete, így elkerülhető az is, hogy a dokumentum aláírója letagadhassa, hogy az adott tartalomhoz köze van.

A digitális aláírás alkalmazásának folyamata a következő: A feladó két kulccsal rendelkezik. Az egyik a titkos kulcs, amelyet a feladó a levél megírása után használ, hogy aláírja az üzenetet (ez alapján tudja azonosítani saját magát), ezután a számítógép készít egy a tartalmat hitelesítő karaktersorozatot (hash- függvényt), ez egy speciális eljárás, amely a levél tartalma alapján készül. Ezután a feladó elküldi a levelet a címzettnek, a címzett a feladó másik kulcsával, a nyilvános kulccsal ellenőrzi, hogy a küldés során nem módosult e a levél és a feladó tényleg az akinek mondja magát. A címzett ezt hash- függvény segítségével tudja ellenőrizni, ha a levél küldés során akár egy karaktert is megváltoztattak, akkor a címzett és a

feladó hash- függvény értéke eltérő lesz. Ez a folyamat látható, leegyszerűsítve a következő ábrán:



8. ábra: Digitális aláírás

Digitális aláírást manapság már nagyon sok helyen használhatunk. Nem csak a polgári életben alkalmazható, hanem már hivatalos ügyeinket is el tudjuk végezni ennek segítségével az Interneten keresztül.

Magyarországon hivatalos ügyeink intézésére fejlesztette ki a magyar állam, az Ügyfélkaput. Az Ügyfélkapun keresztül intéztem el, például egyetemi felvételimet, amelynek segítségével nem kellett postára, bankba és egyéb helyekre mennem, hanem az Interneten keresztül tudtam a banki-átutalásomat és a felvételi jelentkezésemet is elintézni.

4.5. Tanúsítvány, a hitelesítés eszköze

Nyilvános kulcsú rendszereknél (például: digitális aláírás) használjuk a tanúsítványokat. Fontos, hogy a feladó nyilvános kulcsát a címzett hiteles módon ismerje meg. Legjobb, ha a felek személyesen cserélnek nyilvános kulcsokat, de ha ez nem lehetséges, akkor tanúsítvánnyal igazolhatja magát a feladó. Az elektronikus tanúsítványok feladata, hogy a feladó személyes adatait ellenőrizhető módon összekapcsolja a nyilvános kulcsával.

A tanúsítványok tartalmazzák:

1. A tanúsítvány tulajdonosának adatait (név, lakhely, stb.)
2. Nyilvános kulcsát

3. A tanúsítvány érvényességének kezdeti és lejárati időpontját

4. Annak a személynek vagy szervezetnek a nyilvános kulcsát, amely a tanúsítvány valódiságát garantálja (megbízható harmadik fél). Ilyen hitelesítő személy lehet, akiben mindkét fél megbízik vagy olyan független szervezet, amelyben a tanúsítványt felhasználók közössége bízik meg. Ilyen tanúsítvány kiadására jogosult szervezet, például a Verisign, a Netlock vagy a Microsec Kft..

5. Összegzés

Szakdolgozatom célja az volt, hogy betekintést nyújtsak az információmenedzsment területébe, ezen belül az adatvédelem és adatbiztonság informatikai hátterével foglalkoztam a munkám során. Fontosnak tartottam, hogy feltárjam azt, hogy egy vállalat mindennapi működése során milyen veszélyek megelőzésére kell figyelmet fordítani illetve, hogyan védhetjük a vállalat tulajdonában lévő információkat, üzleti titkokat, annak érdekében, hogy ne kerüljenek illetéktelen kezekbe és ne tudjanak vagy nehezebben tudjanak visszaélni velük. Az adatvédelem, adatbiztonság területén fontos, hogy mindig napra készek legyünk, tisztában legyünk a legújabb támadási módszerekkel annak érdekében, hogy a támadási kockázatot csökkenteni tudjuk.

Munkám során kitértem mind a jogi, mind pedig a fizikai, szellemi védelemre, így nem csak a vállalat IT- szolgáltatásait, hanem az egyéb eszközeit is védhetjük. Egy szervezet védelmi rendszerét minden oldalról megvizsgáltam. Megnéztem, hogy ma Magyarországon milyen törvényeket kell betartani, annak érdekében, hogy a személyes adatainkkal, üzleti titkainkkal ne élhessenek vissza. Vizsgáltam, hogy milyen eszközök segítségével előzhetjük meg a különböző katasztrófákat vagy emberi támadásokat, véletlen hibákat. A kockázatelemzés és katasztrófa elhárítás részben kifejtettem, hogy hogyan kell felkészülni a nem kívánt eseményekre. Fontos, hogy minden eshetőséggel számoljunk és a vállalat minden részét felkészítsük, hogy milyen folyamatok elvégzését kell elvégezniük az egyes katasztrófák esetén. Ezeknek a tervezéseknek a célja, hogy minél hamarabb üzemképessé tegyük a szervezetet egy esetleges vis major bekövetkezése esetén, a lehető legköltséghatékonyabb módon.

Szakdolgozatom negyedik részében az adatbiztonság témakörével foglalkoztam. Az adatbiztonság eszközei közé tartoznak a különböző partner-azonosítási eszközök, a különböző titkosítási módok, a digitális aláírás és egyéb eszközök, amelyek segítségével a szoftvereszközök védelme érdekében alkalmazhatunk. A szellemi tulajdonunkat védjük az adatbiztonság eszközeivel, hogy jogtalanul ne juthasson senki a vállalat adataihoz. Ezzel megelőzzük azt, hogy bárki visszaélhessenek az adatokkal, jogtalanul felhasználhassa azt és ezzel előnyt tudjon kovácsolni, például egy konkurens vállalat. Az adatbiztonság fontos részét képezi a vállalati életben, mivel ezzel előzzük meg az adatok illetéktelen kezekbe jutását,

védelmet nyújthat a vállalaton belüli és kívüli támadásokkal szemben is, ennek érdekében a szervezet védelmi rendszerét rendszeresen tesztelni kell és napra kész kriptográfiai eszközöket kell alkalmazni.

Összességében elmondható, hogy az Internet és az egyéb hálózatok rengeteg veszélyt rejtenek, ezért mindig kellő bizalmatlansággal kezeljük ezeket az eszközöket. Fontos, hogy mindig a megfelelő elővigyázatossággal használjunk bármilyen hálózatot. A 21. században az információs társadalom folyamatosan fejlődik, a most felnövekvő nemzedékek a számítógépek világában nőnek fel ennek hatására természetessé és egyre könnyebbé válik, hogy a különböző védelmi eszközöket megpróbálják kijátszani és ez előbb utóbb sikerülni is fog, mivel még százszázalékos biztonság nem létezik csak az elméletben, de addig ameddig a százszázalékos védelmi rendszert feltalálják, addig is megnehezíthetjük a jogosulatlan hozzáférők munkáját.

Irodalomjegyzék

Nyomtatott irodalom

1: Dietz Gusztávné DR.- Pap Mária
Adatvédelem, adatbiztonság
NOVORG (1995)

2: F. Ható Katalin
Adatbiztonság, adatvédelem
Számalk Kiadó (2000)

3: Gábor András
Információmenedzsment
Aula Kiadó (1997)

4: Raffai Mária
Információrendszer-tervezés – Információmenedzsment, fejlesztési módszertanok
Novadat Bt. (1996)

5: Raffai Mária
Az információ - Szerep, hatás, menedzsment
Palatia Nyomda és Kiadó (2006)

Elektronikus irodalom

6: https://wiki.sch.bme.hu/pub/Valaszthato/AdatVedelem/adatv.pdf

7: http://www.civil.dalfold.hu/dokumentumok/EA/szemelyesadatokvedelme.pdf

8: www.kissgaborzsolt.hu/docs/management/ITB_cop03w6.doc

9: http://pcforum.hu/hirek/8755/Ma+35+eves+az+Internet.html

10: http://hu.shvoong.com/social-sciences/communication-media-studies/1966109-az-internet-t%C3%B6rt%C3%A9nete/

11: http://www.szgti.bmf.hu/~mtoth/segedanyagok/Kooperat%A1v2001/DataSecurity.ppt

12: http://old.hungary.com/telecomputer/5_14/04_2kkk.html

13: http://ecdlweb.hu/index.php?title=Elektronikus_al%C3%A1%C3%ADr%C3%A1s,_titkos%C3%ADt%C3%A1s

14: http://www.itb.hu/ajanlasok/a15/html/a15_10-2.htm

15: http://abiweb.obh.hu/abi/index.php?menu=beszamolok/1995-96/IV/2

16: *http://kit2.bdf.hu/epub/hun/palvolgyi/im/im_2fej.rtf*

Ábra