Informatikai Rendszerek Minőségbiztosítása és Auditja

Győrffyné Holló Krisztina
PE informatikai biztonsági szakértő, ISMS lead auditor
NKE phd hallg.
2021.10.08.

Informatikai Rendszerek Minőségbiztosítása és Auditja

Tantárgyi tematika

1. Az információbiztonság, aktualitása, területei; Az információbiztonság alapfogalmai; Az információbiztonság gyakorlati megvalósításának területei; (Információbiztonság)
2. Az információbiztonság szervezete; Az információbiztonság szabályozó dokumentációja; (ISMS)
3. EU és jogszabályi követelmények; GDPR vonatkozások; (hazai és nemzetközi jogszabályok)
4. A védendő információs vagyon meghatározása és kezelése; Az információs vagyon fenyegetettségei, veszélyek;
5. A kockázatmenedzsment, becslésének, elemzésének, értékelésének és kezelésének módszerei;
6. Az üzletmenet-folytonosság és a katasztrófa-elhárítás tervezése (BCP/DRP) és működtetése;
7. A fizikai biztonság és az őrzés-védelem; A hagyományos, papír alapú információk védelme;
8. A személyekkel, emberi erőforrás védelme, infotv és GDPR; Az informatikai védelem;
9. Katasztrófa-elhárítás információbiztonsági vonatkozási; Incidenskezelés;
10. Az információbiztonság működésének ellenőrzése, mérése;
11. Az ISO/IEC 27001 szabvány követelményei és struktúrája;
12. Gyakorlatok, esettanulmányok, ZH

Informatikai Rendszerek Minőségbiztosítása és Auditja I. Információbiztonság

Győrffyné Holló Krisztina
PE informatikai biztonsági szakértő, ISMS lead auditor

Információbiztonság
Szabályozás I

Szabványok:

- ISO/IEC 27000-es szabványcsalád
  - ISO/IEC 27001:2013 (MSZ ISO/IEC 27001:2014)
- ISO/IEC 9001:2015

Nemzeti jogszabályok, vonatkozó rendelkezések, irányelvek:

- a 2011. évi CXII. tv., az információs önrendelkezési jogról és az információszabadságról
- a 2013. évi L. tv., az állami és önkormányzati szervek elektronikus információbiztonságáról
- a 41/2015. (VII. 15.) BM rendelet
- a 2013. évi V. tv., a Polgári Törvénykönyvről
- a 2012. évi C. tv., a Büntető Törvénykönyvről
- Digitális Magyarország, E-közigazgatási keretrendszer koncepció
- 1999. évi LXXVI. törvény a szerzői jogról

Információbiztonság
Szabályozás II

Nemzetközi szabályok:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) - GDPR
- Európai Bizottság: Európai interoperabilitási keret – Végrehajtási stratégia (2017)
- Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről

Információbiztonság
A kezdetek I

Az **Informatikai Biztonsági Irányítási Rendszer** (**IBIR**, angolul Information Security Management System, **ISMS**) az **ISO/IEC 27001:2013** szabványa:

- egy általános irányítási rendszer, amely az üzleti kockázat elemzésén alapul,
- megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az információbiztonságot.
- az IR magában foglalja a szervezetet, a struktúrát, a szabályzatokat, a tervezési tevékenységeket, a felelősségeket, a gyakorlatokat, az eljárásokat, a folyamatokat és az erőforrásokat.

Az **ISO/IEC 27002** ajánlás alapját képezte: **BS 7799**:

- a Brit Szabványügyi Hivatal (British Standard Institute, BSI) által kiadott brit szabvány.
- 1987 májusa, a feladat: nemzetközi szinten is elfogadható informatikai biztonság értékelési és tanúsítási kritériumok és mechanizmus kidolgozása.

  eredménye: az ITSEC, az a UK ITSEC Scheme dokumentumok.

Információbiztonság
A kezdetek II

- Az ITSEC az informatikai rendszerek, informatikai termékek biztonsági funkcióira, valamint ezek biztonsági értékelésére és tanúsítására vonatkozó követelményeket tartalmazza. A UK ITSEC Scheme az értékelési, tanúsítási és minősítési folyamatokat határozza meg.
- A DTI/CCSC* másik feladatában a brit számítógép felhasználók támogatását tűzte ki célul, amely 1989-ben „A Users Code of Practice" címen került kiadásra.
- A **BS 7799** szabvány első revíziója: 1999-ben, és az első részét nemzetközi szabványként (ISO) történő elfogadásra javasolta BSI. A **Nemzetközi Szabványügyi Szervezet** 2000 augusztusában a BS 7799 1. részét változatlan szerkezetben, és gyakorlatilag változatlan tartalommal nemzetközi szabványnak fogadta el **ISO/IEC 17799** néven.
- A **BS 7799**-re alapozott értékelési és tanúsítási folyamatot az Egyesült Királyságban az úgynevezett c:cure eljárásrendben írták le.

*Department of Trade and Industry's, Commercial Computer Security Centre (Kereskedelmi és Ipari Minisztérium, Kerekedelmi Számítógép Biztonsági Központ)

IT Security Evaluation Criteria (Információtechnológiai Biztonság Értékelési Kritériumok)

UK ITSEC Scheme = Egyesült Királyság Információtechnológiai Biztonság Értékelési Kritériumok Eljárásrend

Információbiztonság
A kezdetek III

C:cure - angol séma

- A c:cure-t két évvel az elfogadás után visszavonták.
- Egy alternatív tanúsítási séma, amely az EA7/03, „Útmutató az Akkreditációs Testületeknek, amelyek Információbiztonsági Irányítási Rendszereket tanúsítanak/regisztrálnak" címet viselte, sokkal elfogadottabbá vált az Európai Unióban, mint az angol séma, így Nagy-Britannia is áttért ennek használatára.

ISO 27001-es szabványcsalád

- 2007-ben **ISO/IEC 27001:2007** címmel nemzetközi szabványként is ezt a sémát fogadták el, amelyet 2011-ben ISO/IEC 27001:2011 jelezettel frissítettek.
- Az új magyar kiadás 2013–ban jelent meg.
- 27001-es szabványcsalád – folyamatos fejlesztés, bővítés.

Információbiztonság, Információvédelem

Miért van szükség szabványokra?

Az információ a szervezetek számára a legnagyobb érték.

Az információ megfelelő **védelem nélkül**:

- Ellenőrizetlen az adatok **kiszivárgás**a.
- Az átgondolatlan, ellenőrizetlen módosítások **adatvesztés**t okozhatnak.
- Nyomnélküli adatvesztés esetén kicsi a **helyreállíthatóság** esélye.
- Az információk **nem érhetőek el,** amikor szükség van rájuk.

Az információk megfelelő védelemmel rendelkezzenek.

Információbiztonság Szabványok I

Bizalmasság – Sértetlenség – Rendelkezésre állás elvei

ISO 27000-es szabványcsalád:

- **ISO/IEC 27001:2013, Információbiztonság-irányítási rendszer**
- ISO/IEC 27002:2013, Az információbiztonság irányítási gyakorlatának kézikönyve (Code practice) (útmutató)
- ISO/IEC 27003:2010, Bevezetés (útmutató)
- ISO/IEC 27004:2009, Mérés (biztonsági terület)
- ISO/IEC 27005:2011, Kockázat (biztonsági terület)
- ISO/IEC 27006:2011, Követelmények (auditálás)
- ISO/IEC 27007:2011, IBIR auditálás útmutató
- ISO/IEC 27008:2011, S kontroll audit útmutató

Információbiztonság
Szabványok II

ISO 27000-es szabványcsalád – folyt.

- ISO/IEC 27031:2011, Üzletmenet folytonosság BCP
- ISO/IEC 27033:2009, Hálózatbiztonság (6 rész)
- ISO/IEC 27034:2011, Alkalmazásbiztonság (7 rész)
- ISO/IEC 27035:2011, Incidenskezelés

Információbiztonság
Szabványok III

ISO 9000-es szabványcsalád

- ISO/IEC 9000:2009 – Minőségirányítási rendszerek, Alapok és szótár
- ISO/IEC 9001:2015 – Minőségirányítási rendszerek, követelmények
- ISO/IEC 9004:2009 – A szervezet tartós sikerének irányítása. Minőségirányítási megközelítés.

Információbiztonság
ISO/IEC 9001:2015 szabvány (ISO/IEC 27001:2013)

- **Revolúciós** jellegű változások.
- Kevésbé leíró jellegű, inkább a **teljesítményre** koncentrál.
- **Folyamatszemléletű** megközelítést ötvözték a kockázatalapú szemlélettel.
- A szervezet minden szintjén alkalmazzák a **PDCA** ciklust.
- Cél: az irányítási rendszerszabványok **egységes szerkezet**ének kialakítása.

Információbiztonság
ISO/IEC 27001:2013 szabvány

Fejezetei:

- Alkalmazási terület
- Rendelkező hivatkozások
- Szakkifejezések és meghatározások
- A szervezet környezete
- Vezetés
- Támogatás
- Működés
- Teljesítményértékelés
- Fejlesztés

Információbiztonság
ISO/IEC 27001:2013 szabvány

Fontosabb fogalmak I:

- **Vevőközpontúság**: A szervezetek vevőiktől függenek, ezért ismerniük kell a jelenlegi és a jövőbeli vevői szükségleteket, teljesíteniük kell a vevők követelményeit, és igyekezniük kell felülmúlni a vevők elvárásait.
- **Vezetés**: A vezetők megteremtik a szervezet céljainak és igazgatásának egységét. Hozzanak létre és tartsanak fenn olyan belső környezetet, amelyben a munkatársak teljes mértékig részt vehetnek a szervezet céljainak elérésében.
- A **munkatársak bevonása**: A szervezet lényegét minden szinten a munkatársak jelentik, és az Ő teljes mértékű bevonásuk teszi lehetővé képességeik kihasználását a szervezet javára.
- **Folyamatszemléletű megközelítés**: A kívánt eredményt hatékonyabban lehet elérni, ha a tevékenységeket és a velük kapcsolatos erőforrásokat folyamatként irányítják.

Információbiztonság
ISO/IEC 27001:2013 szabvány

Fontosabb fogalmak II:

- **Rendszerszemlélet** az irányításban: Az egymással összefüggő folyamatok rendszerként való azonosítása, megértése és irányítása hozzájárul ahhoz, hogy a szervezet eredményesen és hatékonyan valósítsa meg céljait.
- **Folyamatos fejlesztés**: A szervezet teljes működésének átfogó, folyamatos fejlesztése legyen a szervezet állandó célja.
- **Tényeken alapuló döntéshozatal**: Az eredményes döntések az adatok és egyéb információ elemzésén alapulnak.
- **ISO/IEC 27001:2013 A melléklet!**

Információbiztonság
ISO/IEC 27001:2013 szabvány

Egyéb **jellemzők**:

- Nem kötelező érvényű, minden alkalmazó önként vállalja e szabvány követelményeinek teljesítését.
- A követelményeket általánosan fogalmazza meg.
- Nemcsak a termelő és szolgáltató szervezetekre alkalmazható.
- A piac által vezérelt szabvány, vevőorientált.
- Információbiztonsági követelmények.

Információbiztonság
ISO/IEC 27001:2013 szabvány

Bevezetés **előny**e:

- A **nemzetközi információbiztonsági előírásoknak** való megfelelés.
- Előnyök: **versenyelőny** a piacon,
- **Szabályozottság**: szabályozottabb termelés, szolgáltatás, működés,
- **Irányítás**: jobb, pontosabb vezetői információk,
- **Hatékonyság**: hatékonyabb irányítás és munkavégzés, javul a belső működés hatékonysága, szervezettsége,
- **Költséghatékonyság**: csökkennek az üzemeltetési költségek,
- **Ösztönzés**: ösztönző hatást gyakorol a beszállítói körre,
- **Fejlődés**: kialakul a folyamatos fejlődés igénye.

Információbiztonság
ISO/IEC 27001:2013 szabvány, rendszeraudit

Bevezetés előkészítése:

- A vállalkozás tevékenységi folyamatainak, eljárásainak, ügymenetének **felmérése**.
- Szervezeti **átvilágítás**.
- A rendelkezésre álló **dokumentáció** átvizsgálása.
- Minőségügyi és információbiztonsági **tréning** a társaság vezetői, a kijelölt megbízott, valamint a rendszer kiépítésében közreműködő dolgozók számára.
- A működőképes információbiztonsági irányítási rendszer kiépítéséhez szükséges **erőforrások** meghatározása.

Információbiztonság
ISO/IEC 27001:2013 szabvány, rendszeraudit

Az információbiztonsági irányítási **dokumentumrendszer** kidolgozása

- Információbiztonsági politika és célok
- Információbiztonsági irányítási kézikönyv, szabályzat (ISZ és IBSZ)
- Eljárások és utasítások
- Munka- és vizsgálati utasítások
- Bizonylatok, formanyomtatványok, űrlapok

Információbiztonság
ISO/IEC 27001:2013 szabvány, rendszeraudit

Az információbiztonsági irányítási rendszer **bevezetés**e:

- Információbiztonsági tréningek
- Irodai és fizikai rendteremtés (dokumentumok és eszközök védelme, biztonsága)
- Hitelesítések, kalibrálások elvégeztetése
- Belső IT auditorok képzése
- Belső IT auditok bonyolítása
- A szükséges megelőző és helyesbítő intézkedések meghatározása, végrehajtása

Információbiztonság
ISO/IEC 27001:2013 szabvány, rendszeraudit

A **tanúsítás folyamata**:

- Előaudit (nem kötelező, választható)
- Dokumentáció vizsgálat
- Helyszíni audit
- Auditjelentés

Információbiztonság
ISO/IEC 27001:2013 szabvány

PDCA elv

- **Bevezette**: Organistaion for Economic Co-Operation and Development – OECD (Gazdasági Együttműködési és Fejlesztési Szervezet)
- W.E. Demingről elnevezett Deming ciklus (Deming's Cycle)
- **Folyamatmodell** az IR fejlesztésének, megvalósításának és hatékonyságának biztosítására
- Lefedik a teljes tevékenységi ciklust.
- Bármilyen műveletre, tevékenységre, folyamatra, rendszerre, működtetésre, koncepcióra, elgondolásra vonatkoztatható, zárt hatásláncú, folytonosan ismétlődő **körfolyamat-elv**.

Információbiztonság
ISO/IEC 27001:2013 szabvány

PDCA elv

- első szakasz a **Tervezés** (**Plan**) – a fennálló helyzet tanulmányozása, adatgyűjtés, javítás megtervezése
- második szakasz a **Végrehajtás** (**Do**) – a terv kipróbálása kísérleti jelleggel egy kisebb projekt vagy a felhasználók egy szűkebb körén belül alkalmazva
- harmadik szakasz az **Ellenőrzés** (**Check**) – a változtatások hatásának elemzése és értékelése)
- negyedik szakasz a **Beavatkozás** (**Act**) – a bevált módszer bevezetése és szabványosítása

Információbiztonság
ISO/IEC 27001:2013 szabvány

MSZ ISO/IEC 27001:2014 (ISO/IEC 27001:2013) szabvány

Informatikai Biztonsági Irányítási Rendszer (IBIR)

(Information Security Management System, ISMS)

- **Általános** irányítási rendszer, amely az üzleti kockázat elemzésén alapul.
- **Megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az információbiztonságot**.

Információbiztonság
ISO/IEC 27001:2013 szabvány

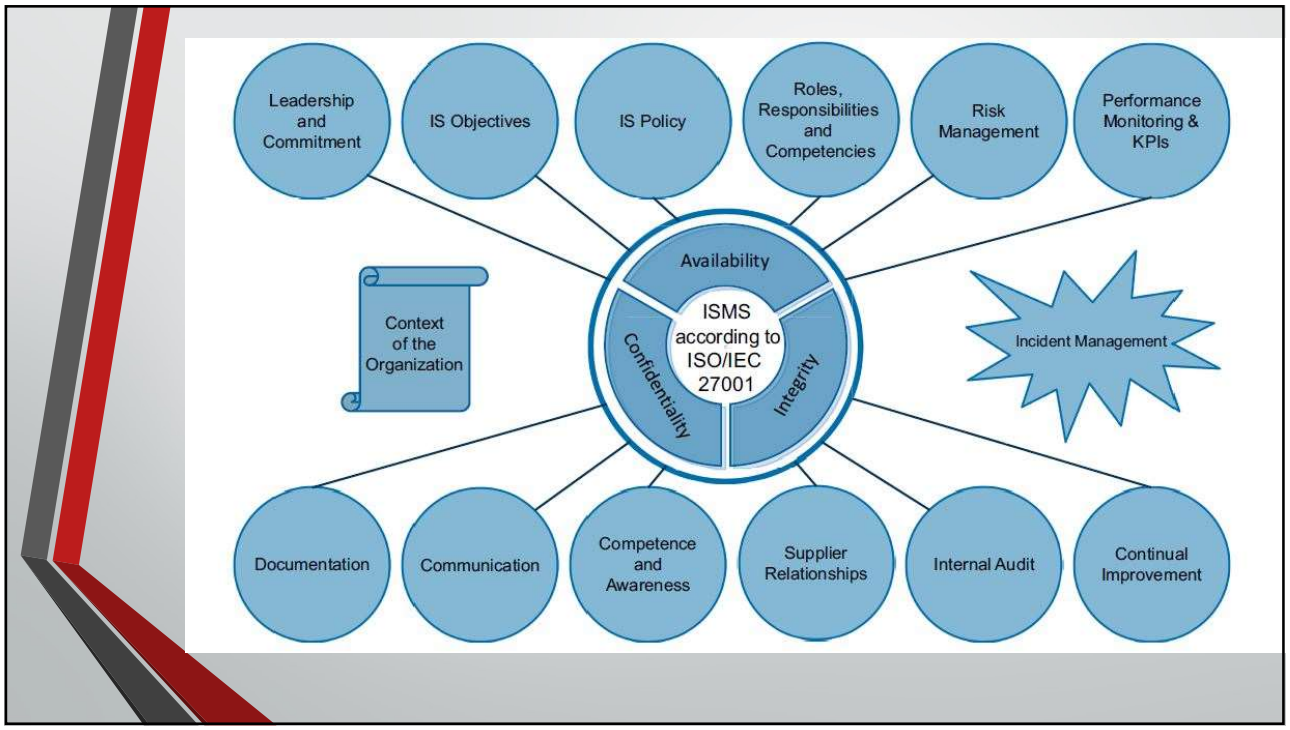
Követelményrendszer az Információbiztonsági Irányítási Rendszer

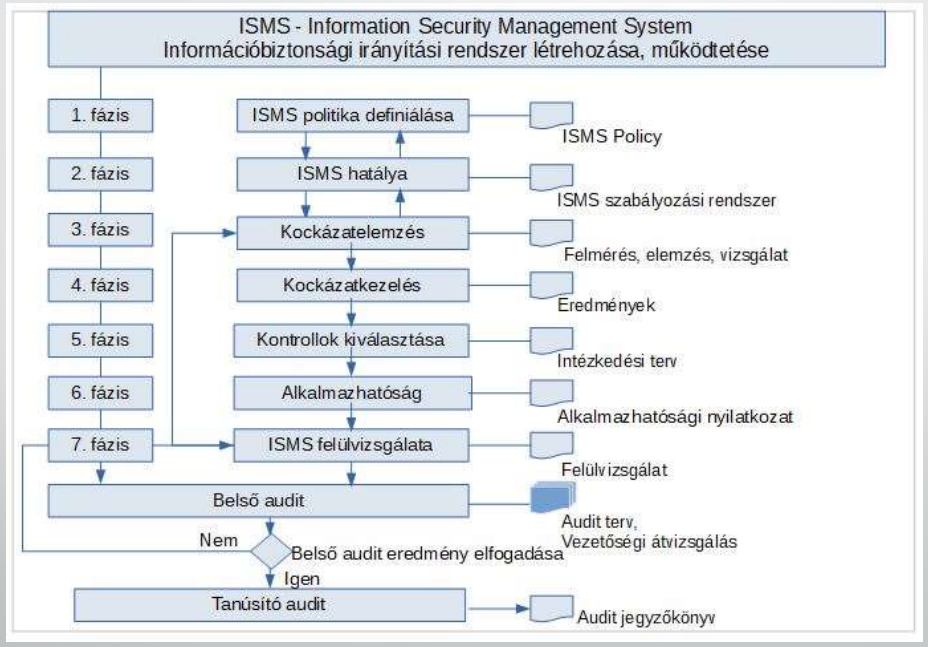
- tervezéséhez,
- létrehozásához,
- ellenőrzéséhez és
- bevezetéséhez

az informatikai biztonsági rendszer teljes életciklusában bekövetkező tevékenységekre vonatkozólag.

Informatikai Rendszerek Minőségbiztosítása és Auditja II. Információbiztonság irányítási rendszer

ISO/IEC 27001:2013 szabvány
Tervezés és bevezetés





Információbiztonsági irányítási rendszer
Alkalmazási terület

Követelmények:

Információbiztonsági kockázatoknak a szervezet igényeihez igazodó

- felmérésére és
- kezelésére.

ISO/IEC 27001:2013 (MSZ ISO/IEC 27001:2014) szabvány, A melléklet !

Nemzetközi tanúsítás esetén a teljes szabvány követelményrendszer alkalmazása kötelező, követelmény kizárás nem lehetséges.

Információbiztonsági irányítási rendszer
Tervezés és bevezetés I

Meghatározások I.

- A szervezet és környezete:
  - Külső és belső tényezők
  - Érdelelt felek igényei és elvárásai (jogi szabályozás is!)
  - Alkalmazási terület
  - IBIR létrehozása
- Vezetés
  - Vezetőségi elkötelezettség, Információbiztonsági nyilatkozat
  - Információbiztonsági politika
  - Szervezeti szereplők, felelősségek és hatáskörök

Információbiztonsági irányítási rendszer
Tervezés és bevezetés II

Meghatározások II.

- Tervezés
  - Kockázatmenedzsment
  - Információbiztonsági célok és azok elérésének ütemezése
- Támogatás
  - Erőforrás
  - Felkészültség
  - Tudatosság
  - Kommunikáció
  - Dokumentált információ

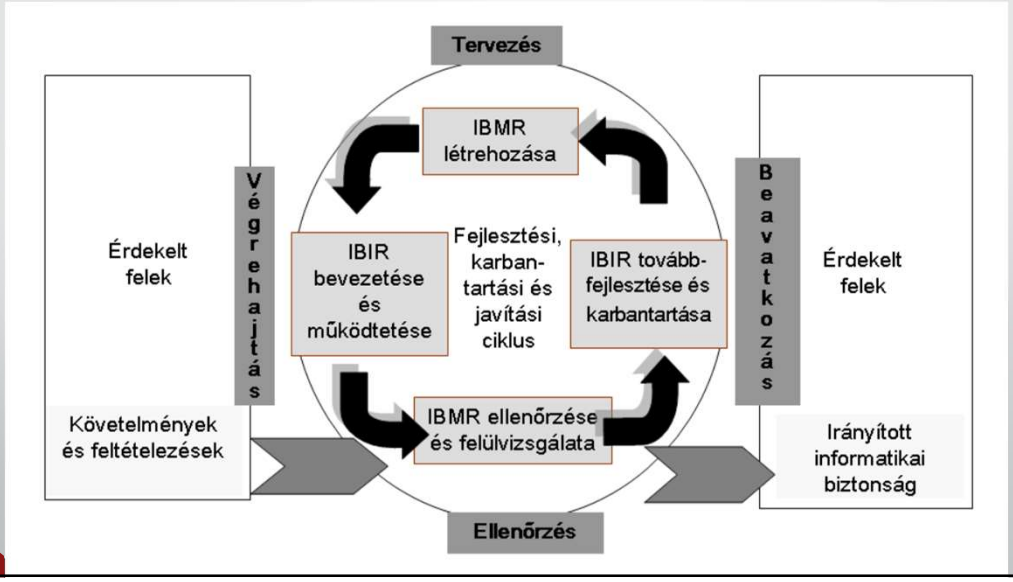
Információbiztonsági irányítási rendszer
Tervezés és bevezetés III

Meghatározások III.

- Működés
  - Tervezés és felügyelet
  - Kockázatfelmérés
  - Kockázatkezelés
- Teljesítményértékelés
  - Megfigyelés, mérés, elemzés és értékelés
  - Belső audit

Információbiztonsági irányítási rendszer
Tervezés és bevezetés IV

PDCA



Információbiztonsági irányítási rendszer
PDCA elv

- **Tervezés** (IBIR létrehozása, Plan): A szervezet általános szabályainak megfelelő **biztonságpolitika, célok, módszerek, folyamatok** és **eljárások** meghatározása, amelyek relevánsak a kockázatkezelés és az informatikai biztonság fejlesztése szempontjából.

- **Végrehajtás** (IBIR bevezetése és működtetése, Do): A biztonsági szabályzat, intézkedések, módszerek és eljárások megvalósítása és üzemeltetése.

- **Ellenőrzés** (IBIR ellenőrzése és felülvizsgálata, Check): Fel kell becsülni és – ahol alkalmazható – fel kell mérni a biztonságpolitika végrehajtásának folyamatát, a célok és a gyakorlati tapasztalatok alapján az eredményeket a vezetés számára jelenteni kell.

- **Beavatkozás** (IBIR továbbfejlesztése és karbantartása, Act): A vezetői felülvizsgálat eredményén alapuló korrigáló és megelőző intézkedéseket kell hozni, illetve folyamatosan tovább kell fejleszteni a Rendszert.

Információbiztonsági irányítási rendszer
Bevezetés - helyzetfelmérés

- Szabályozási környezet
- Szervezeti biztonság
- Vagyontárgyak biztonsága
- Emberi erőforrások biztonsága
- Fizikai és környezeti biztonság
- A kommunikáció és üzemeltetés biztonsága
- Hozzáférés-ellenőrzés
- Fejlesztés, beszerzés, karbantartás
- Incidenskezelés
- Működés folytonosságának irányítása
- Megfelelés (jogszabályi, törvényi)

Információbiztonsági irányítási rendszer
Bevezetés - helyzetfelmérés, segédeszközök

Módszerek:

COBIT
- relatív mérce, hogy hol tart a vállalkozás
- hatékony eldöntéshez, célok eléréséhez
- mérhető az előrehaladás

CRAMM

ITB

MARION

IT – Grundschutzhandbuch

Információbiztonsági irányítási rendszer
Bevezetés – meghatározás és dokumentálás

A szervezet

A szervezet és környezete:

- Külső és belső tényezők
- Érdelelt felek igényei és elvárásai (jogi szabályozás is!)
- Alkalmazási terület
- IBIR létrehozása, definiálása, terület és kiterjedés meghatározása

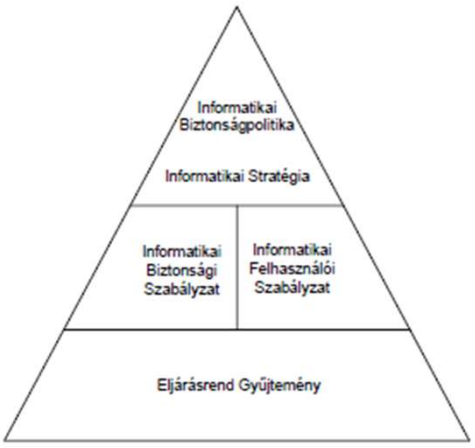
Információbiztonsági irányítási rendszer
Bevezetés – meghatározás és dokumentálás

A **Vezetés**

- Vezetőségi elkötelezettség, Információbiztonsági nyilatkozat

  (szándéknyilatkozat a bevezetésre és a működtetésre)

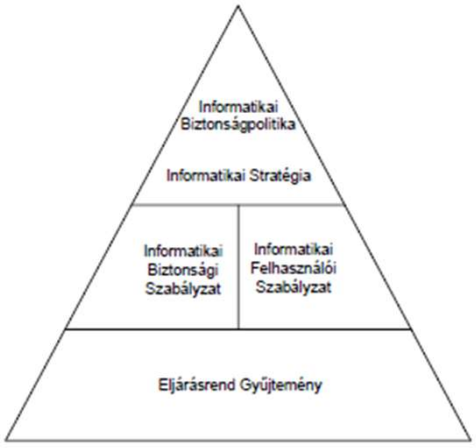
- Információbiztonsági politika
- Szabályzat: ISZ, IBSZ, IFSZ
- Eljárások
- Informatikai Stratégia (IFT)
- Szervezeti szereplők, felelősségek és hatáskörök



Információbiztonsági irányítási rendszer
Bevezetés – Információbiztonsági politika

- Felső vezetői jóváhagyás, kiadás és közzététel
- Biztonság iránti elkötelezettség
- Biztonsági célok
- Magas szintű biztonsági elvárások
- Védelmi intézkedések specifikálásának és kialakításának alapja
- Figyelemmel kísérés és fejlesztés
- Befolyásoló tényezők:

  Környezet, szervezeti és kulturális tényezők



Információbiztonsági irányítási rendszer
Bevezetés – Információbiztonsági politika

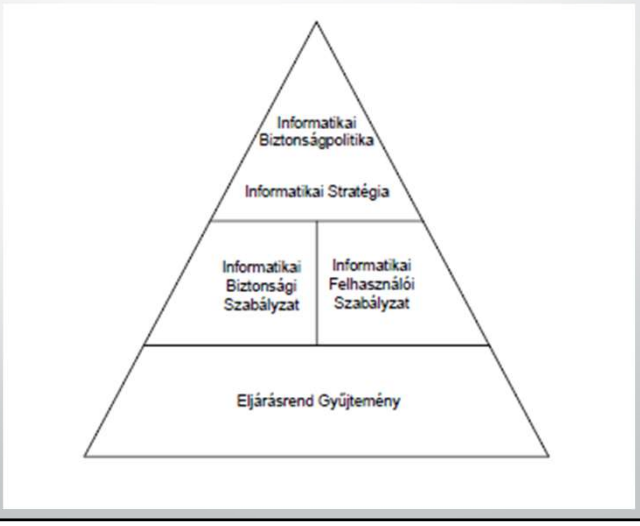
Általános irányelvek:

- a hitelesség biztosítása,
- a bizalmasság biztosítása,
- a sértetlenség biztosítása,
- a rendelkezésre állás,
- a biztonsági osztályba sorolás és
- a működőképesség fenntartása.

Információbiztonsági irányítási rendszer
Bevezetés – Információbiztonsági politika

Kialakításkor bevonható **területek**

- (felső)vezetés
- biztonság - vagyonvédelem
- informatika
- belső ellenőrzés
- pénzügy - kontrolling
- épületfenntartás és infrastruktúra-üzemeltetés
- humán erőforrás menedzsment
- minőségirányítás



Információbiztonsági irányítási rendszer
Bevezetés – Információbiztonsági politika

Következő **iránymutatásokat** foglalja magába:

- az informatikai biztonságpolitika **kiterjedését és célját,**
- az informatikai biztonság **meghatározását,** általános célkitűzéseit és tárgykörét, valamint a biztonság fontosságát,
- a vezetőség **szándéknyilatkozatát,** amely támogatja az informatikai biztonság céljait és elveit,
- az informatikai biztonság **szervezési elv**eit, ide értve a szervezeti struktúrát, a személyi felelősségeket és hatásköröket,
- a szervezet tulajdonában levő **adatvagyon elemeinek érzékenységét,** az ennek megfelelő védelmi szinteket, és a **biztonsági osztályozási rendszert,** továbbá – ha van ilyen – az osztályba sorolástól eltérő védelmi igényű adatkörök védelmére vonatkozó politikát,

Információbiztonsági irányítási rendszer
Bevezetés – Információbiztonsági politika

További **iránymutatások**at foglalja magába:

- a kockázatok felmérésére és kezelésére vonatkozó elveket,
- a belső személyzettel és a külső partnerekkel kapcsolatos biztonságpolitikát,
- az informatikai biztonsági ellenőrzés rendszerét,
- az informatikai biztonsági feladatok megosztására vonatkozó elveket,
- a biztonságpolitika változásának ellenőrzési eljárását és felülvizsgálatának körülményeit.

Információbiztonsági irányítási rendszer
Bevezetés – Információbiztonsági politika

Minta:

- Mi a szervezet célja?
- Az elvárás megvalósításához milyen eszközök szükségesek?
- Szervezeti elkötelezettség a rendszer bevezetése és működtetése a .... nemzetközi szabvány alapján. Jogszabályi elkötelezettség.
- Mi a vezetői döntés? (működés, fenntartás, folyamatos fejlesztés tekintetében)
- A szervezet ennek érdekében milyen folyamatokat szabályoz és hajt végre? (folyamatok és szervezeti elkötelezettség a végrehajtandó folyamatok iránt)
- Milyen az erőforrásigénye?

Információbiztonsági irányítási rendszer
Bevezetés – Informatikai Biztonsági Stratégia

Célja:

- a szervezet üzleti igényeinek jövőbeni változásaival összhangban meghatározza az információbiztonság fejlesztésének tervét:
  - rövidtávú,
  - középtávú,
  - hosszú távú.
- dokumentáció a beszerzési, beruházási és projekt-előkészítési tevékenységeket érintő intézkedési tervekhez.

Információbiztonsági irányítási rendszer
Bevezetés – Informatikai Biztonsági Stratégia

Az információbiztonsági stratégia meghatározásánál a szervezetnek:

- fel kell mérnie, ismernie kell a jelenlegi információbiztonsági helyzetét,
- számba kell vennie mindazon biztonsági kihívásokat, melyekkel a közeljövőben számolnia kell, valamint
- fel kell mérnie a biztonság területén lehetséges fejlesztési potenciálokat,
- rögzíteni kell a szervezetre vonatkozó információbiztonsági követelményeket és eljárásokat.

Informatikai Rendszerek Minőségbiztosítása és Auditja III. Információbiztonsági irányítási rendszer, jogszabályok

Nemzeti jogszabályok

Nemzeti jogszabályok, vonatkozó rendelkezések, irányelvek:

- a 2011. évi CXII. tv., az információs önrendelkezési jogról és az információszabadságról (infotv)
- a 2013. évi L. tv., az állami és önkormányzati szervek elektronikus információbiztonságáról (ibtv)
- a 41/2015. (VII. 15.) BM rendelet (bizt. osztály és fok)
- a 2013. évi V. tv., a Polgári Törvénykönyvről (ptk)
- a 2012. évi C. tv., a Büntető Törvénykönyvről (btk)
- Digitális Magyarország, E-közigazgatási keretrendszer koncepció
- 1999. évi LXXVI. törvény a szerzői jogról

Nemzetközi szabályozás - GDPR

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE

(2016. április 27.)

a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

(http://eur-lex.europa.eu)

Nemzetközi szabályozás - GDPR

Szabályozó elemei:

- Természetes személyek személyes adatai, védelme és biztonsága
- Természetes személyek különleges adatai, védelme és biztonsága
- Természetes személyek személyes adatainak kezelése – adatkezelő
- Természetes személyek személyes adatainak feldolgozása – adatfeldolgozó
- Természetes személyek személyes adatainak továbbítása
- Profilalkotás
- Adatgyűjtés
- Adattárolás
- Törlési jog
- Tájékoztatáshoz való jog; hozzáférési, helyesbítési és törlési jog; adathordozhatósághoz való jog, a tiltakozáshoz való jog, a profilalkotáson alapuló döntések és az adatvédelmi incidens érintettel történő közléssel kapcsolatos jog.

Nemzetközi szabályozás - GDPR

További elemek:

- Adatvédelmi hatásvizsgálat (kötelező)

A természetes személyek jogaira és szabadságaira nézve magas kockázattal járó ilyen esetekben az adatkezelő – annak érdekében, hogy az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve felmérje a magas kockázat különös valószínűségét és súlyosságát – az adatkezelés előtt adatvédelmi hatásvizsgálatot végez. Ez a hatásvizsgálat magában foglalja különösen az említett kockázat mérséklését, a személyes adatok védelmét, valamint az e rendeletnek való megfelelés bizonyítását célzó tervezett intézkedéseket, garanciákat és mechanizmusokat.

- Magatartási kódexek létrehozása
- Átláthatóság: olyan tanúsítási mechanizmusok, és adatvédelmi bélyegzők illetve jelölések létrehozása, amelyek lehetővé teszik az érintettek számára, hogy gyorsan értékelni tudják az adott termékek és szolgáltatások adatvédelmi szintjét.

Nemzetközi szabályozás - GDPR

Adatvédelmi tisztviselő:

Az adatvédelmi tisztviselő legalább a következő feladatokat ellátja:

a) tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

b) ellenőrzi az adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;

d) együttműködik a felügyeleti hatósággal; és

e) az adatkezeléssel összefüggő ügyekben kapcsolattartóként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

Nemzetközi szabályozás - GDPR

Adatvédelmi hatásvizsgálat

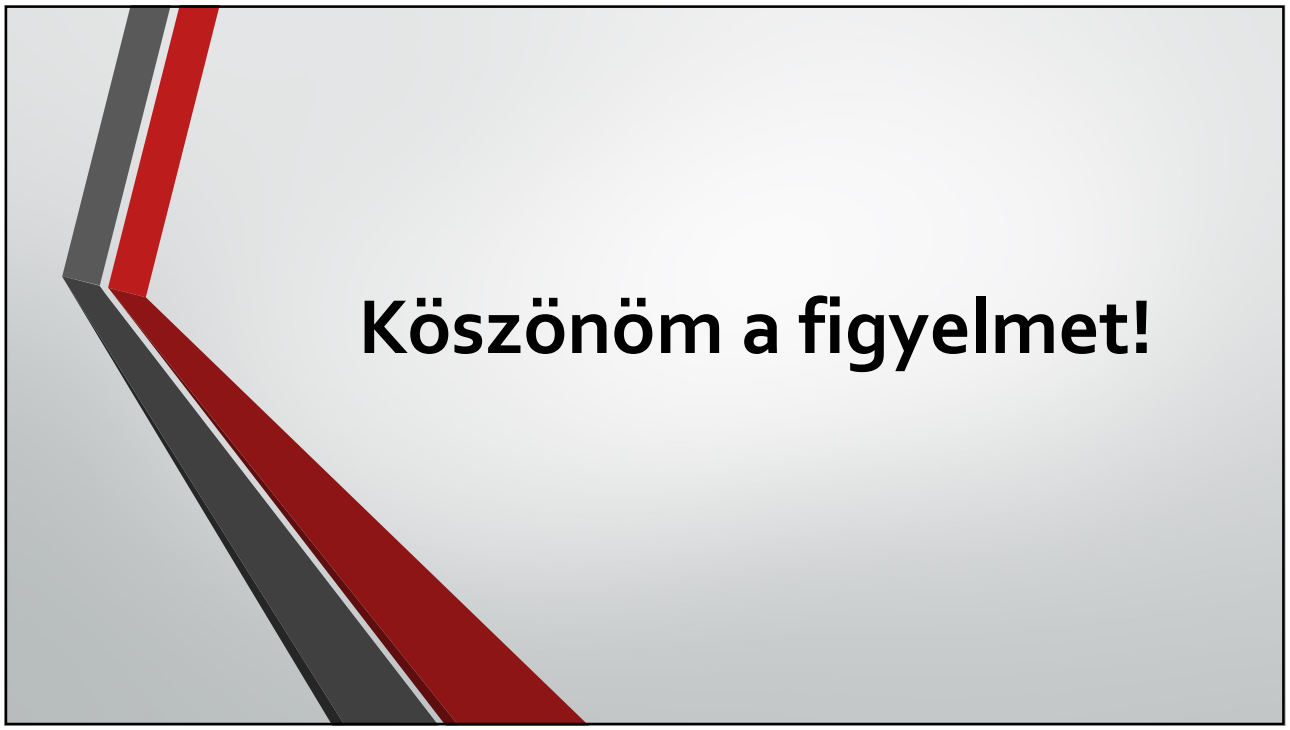
Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

a) természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is –alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;

b) a személyes adatok különleges kategóriái, vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy

c) nyilvános helyek nagymértékű, módszeres megfigyelése.


Köszönöm a figyelmet!

Informatikai Rendszerek Minőségbiztosítása és Auditja II.

Győrffyné Holló Krisztina
PE informatikai biztonsági szakértő, ISMS lead auditor
2021.10.08.

Témák

- EU és jogszabályi követelmények; GDPR vonatkozások; (hazai és nemzetközi jogszabályok)
- Információbiztonsági alapfogalmak (jogszabályok és az ISO 27001 szabvány alapján)
- 4. (témakör a tematika szerint) A védendő információs vagyon meghatározása és kezelése; Az információs vagyon fenyegetettségei, veszélyek
- Esettanulmány (gyakorlat)

Nemzeti és nemzetközi előírások

- a 2011. évi CXII. tv., az információs önrendelkezési jogról és az információszabadságról (infotv)
- a 2013. évi L. tv., az állami és önkormányzati szervek elektronikus információbiztonságáról (ibtv)
- Az európai parlament és a tanács (eu) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (http://eur-lex.europa.eu) (GDPR)

Informatikai Rendszerek Minőségbiztosítása és Auditja Információbiztonsági alapfogalmak

Győrffyné Holló Krisztina

PE informatikai biztonsági szakértő, ISMS lead auditor

Információbiztonsági alapfogalmak Adatműveletek I.

- **Adat**: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;
- **Információ**: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;
- **Adatgazda**: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik;
- **Adatkezelés**: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. Ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;
- **Adatkezelő**: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

Információbiztonsági alapfogalmak Adatműveletek II.

- **Adatfeldolgozás**: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik;
- **Adatfeldolgozó**: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;
- **Adattovábbítás**: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
- **Adattörlés**: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
- **Adatzárolás**: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.

Információbiztonsági alapfogalmak Adatvédelem I.

- **Fizikai védelem:**

zárak, beléptető rendszerek, tűzjelző rendszerek, biztonsági kamerák és őrök

- **Logikai védelem:**

titkosítási algoritmusok, kommunikációs protokollok, tűzfalak, stb.

- **Adminisztratív védelem:**

kockázatmenedzsment, biztonsági szabályzatok, szabványok és ajánlások, törvényi szabályozás.

Információbiztonsági alapfogalmak Adatvédelem II.

- **Adminisztratív védelem**: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;
- **Auditálás**: előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;
- **Fenyegetés**: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;
- **Fizikai védelem**: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;
- **Folytonos védelem**: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

Információbiztonsági alapfogalmak Adatvédelem III.

- **Megelőzés**: a fenyegetés hatása bekövetkezésének elkerülése;
- **Korai figyelmeztetés:** valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;
- **Teljes körű védelem**: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;
- **Védelmi feladatok**: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;
- **Kibervédelem**: a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;
- **Zárt védelem**: az összes számításba vehető fenyegetést figyelembe vevő védelem.
- **Adatvédelmi incidens**: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

Információbiztonsági alapfogalmak Alapelvek - CIA

- **Bizalmasság - C = Confidentiality**: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;
- **Sértetlenség - I = Integrity**: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;
- **Rendelkezésre állás - A = Availability**: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

Információbiztonsági alapfogalmak Adatbiztonság I.

- **Biztonsági esemény**: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;
- **Biztonsági osztály**: az elektronikus információs rendszer védelmének elvárt erőssége;
- **Biztonsági osztályba sorolás**: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;
- **Biztonsági szint**: a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;

Információbiztonsági alapfogalmak Adatbiztonság II.

- **Kiberbiztonság**: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés működtetéséhez;

Információbiztonsági alapfogalmak Kockázatmenedzsment

- **Kockázat**: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;
- **Kockázatelemzés**: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;
- **Kockázatkezelés**: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;
- **Kockázatokkal arányos védelem**: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

Informatikai Rendszerek Minőségbiztosítása és Auditja IV. Az információs vagyon

Győrffyné Holló Krisztina

PE informatikai biztonsági szakértő, ISMS lead auditor

A védendő információs vagyon meghatározása és kezelése

IT biztonság szempontjából a vagyonelemek csoportosítása:

- Hardver
- Szoftver
- Információ/ adat

Információtípus (27001) / adattípus (tv.)

- személyes adat
- különleges adat
- bűnügyi személyes adat

Az információs vagyon nem csak magukat a védendő adatokat foglalja magába, hanem az azokat tartalmazó adat-hordozókat, az adat-átalakító, -továbbító, és -feldolgozó eszközöket, rendszereket (és dokumentációit), amelyeken keresztül az adatok elérhetők, illetve biztonságuk sérülhet. Tágabb értelemben az információs vagyonba beleértendők azok a kommunikációs és védelmi rendszerek is, amelyek az adatvagyon biztonságát hivatottak (közvetve vagy közvetlenül) védeni.

A védendő információs vagyon meghatározása és kezelése

Adatkategóriák

Csoportok meghatározása:

- alaptudományi információ (eredmények alapján), pl.: fizikai, informatikai
- szakterületi (orvosi, műszaki) információ: munkával, termeléssel, üzemeltetéssel kapcsolatos adatok, ismeretek - pl.: fizikai kísérletek eredményei
- statisztikai információ: olyan jel vagy adat, amely statisztikai műveletek eredményeképpen jön létre - pl.: népszámlálási adatok változása
- számviteli információ - az intézmények gazdasági-pénzügyi helyzetéről adnak felvilágosítást - pl.: éves mérleg
- marketing információ - a termékekre és szolgáltatásra, valamint azok piaci helyzetére és a piac résztvevőire vonatkozó ismeretek - pl.: felhasználói igények

A védendő információs vagyon meghatározása és kezelése

Biztonsági osztályok és szintek meghatározása:

- 2013. évi L. tv. és a Nemzeti Elektronikus Információbiztonsági Hatóság (http://neih.gov.hu/urlapok)
- ISO/IEC 27001:2013 IBIR szabvány alapján (ITB kérdéslista)

Szubjektív vagy részlegesen objektív!

Adatkategóriák eredmény:

nyílt, normál v. alap, kiemelt, kritikus biztonsági kategóriák

Az információs vagyon fenyegetettségei, veszélyei

- Sérülékenység (Vulnerability): az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat. Biztonsági rés vagy gyengeség, amely incidensre vagy katasztrófára ad lehetőséget.
- o-day (zéró-day) sérülékenységek: olyan hiba, melyre a gyártó még nem adott ki javítást. Különösen nagy veszélyt jelenthetnek, elterjedtségüktől és kihasználhatóságuktól függően.

Az információs vagyon fenyegetettségei, veszélyei

- Fenyegetés (Threat): olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztás alapú cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát.
- Veszély: olyan személy vagy körülmények együttese, mely biztonsági esemény okozója lehet.
- Katasztrófa (árvíz, tűz, elhagyott biztonsági mentés) vagy támadó (pl. hacker kívülről, belső alkalmazott, vagy robot).

Az információs vagyon fenyegetettségei, veszélyei

Fenyegetés (Threat):

- Külső fenyegetések (External Threats): a támadónak nincs hozzáférése a rendszer belső erőforrásaihoz (hálózat, szerver, végpontok), csak a kívülről publikusan elérhető információkat, szolgáltatásokat látja és a sérülékenységet kihasználva hozzáfér a belső erőforrásokhoz.
- Belső fenyegetések (Internal Threats): a támadó hozzáfér bizonyos belső erőforrásokhoz, pl. tipikusan egy felhasználói fiókhoz (gyenge jelszó), belső hálózathoz vagy csupán a biztonsági eljárások gyakorlatához. A támadó célja lehet jogosultságának kiterjesztése (Privilage Escalation), a privilegizált accunthoz is hozzáférést szerezzen.
  Pl: alkalmazottak, vagy sértődött alkalmazottak (elbocsájtás, bérfeszültség), szerződéses partnerek (szerződésszegés).

Veszélyek I.

Malicious Soft**ware** = Rosszindulatú kód, szoftver, például:

- Vírus (általában fájlhoz kötődő kártevő)
- Féreg (a vírussal szemben önállóan terjed)
- Trójai (más hasznos programnak adja ki magát)
- Rootkit (a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök, melyek pl. hátsóajtót /Backdoor/ nyitnak a támadónak.)
- Kémprogram (Spyware)
- Ransomware (váltságdíjat követelő program)
- Aggresszív reklámprogram (Adware)
- Billentyűzetfigyelő (Keylogger)
- Betárcsázó (Dialer)
- Bot (támadó által irányított zombi-gépek hálózatának (botnet) kliens programja). Célja lehet:
  - további malwerek terjesztése (megrendelésre is)
  - kémkedés
  - spam (levélszemét) küldése
  - DDoS (Distributed Denial of Service) támadás
  - számítások (jelszótörés, BitCoin bányászat, stb.)

Veszélyek II.

Adathalászat:

- Phishing (klasszikus adathalászat)
- Smishing (SMS-en keresztül történő adathalászat)
- Vishing (telefonon keresztül történő adathalászat)
- Pharming (eltérítéses adathalászat)
- Whaling (felső- és középvezetőket megcélzó adathalászat)

Humán alapú technikák:

- Megtévesztés, megszemélyesítéses támadások
- Telefonon keresztüli megtévesztés
- Shoulder surfing (bizalmas információ begépelésének kifigyelése)
- Piggybacking (belépési jogosultság kölcsönzése)
- Tailgating (szoros követés)
- Dumpster diving (hulladék átvizsgálás)

Informatikai Rendszerek Minőségbiztosítása és Auditja Esettanulmány (gyakorlat)

Győrffyné Holló Krisztina
PE informatikai biztonsági szakértő, ISMS lead auditor

Információbiztonsági alapfogalmak Esettanulmány (gyakorlat)

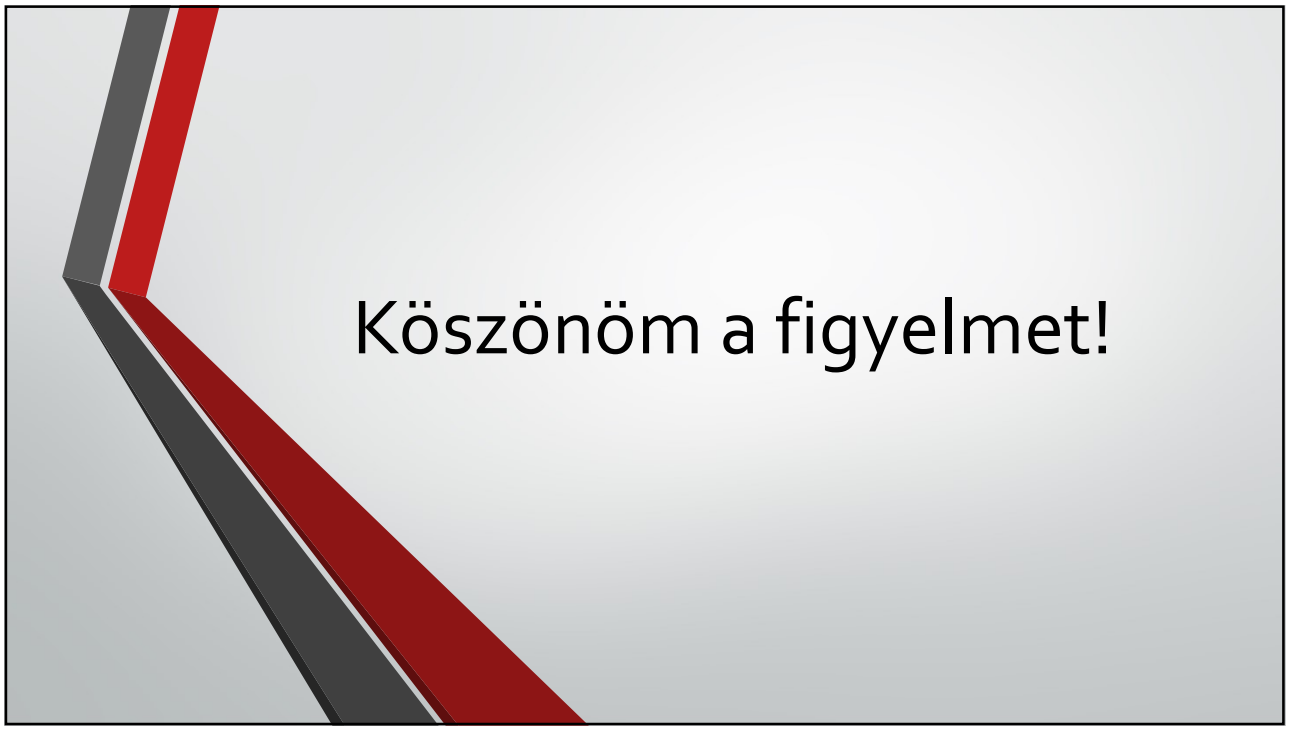
Adattárolás a Data&Service Kft-nél (ISO/IEC 27001:2013 A kommunikáció és az üzemeltetés irányítása; Biztonsági mentés)

Esetleírás (a kapott leírás alapján, részlet):

- A Data&Service Kft. szórakoztatóelektronikai és háztartási gépek szervizelésével foglalkozik. Több márkakereskedőnek a márkaszervize is. Budapesten 3 üzletük van, és az ügyfélszolgálaton keresztüli megrendelésre kimennek ügyfelekhez is a helyszínre…

Feladat:

- Készítse el az esetleírás alapján a lehetséges információkategóriákat!
- Készítsen az információkategóriához adatvagyonlistát, a lehetséges adatvagyon elemekkel!


Köszönöm a figyelmet!

Informatikai Rendszerek Minőségbiztosítása és Auditja III.

Győrffyné Holló Krisztina
PE informatikai biztonsági szakértő, ISMS lead auditor
2021.10.08.

Témák

- 5. A kockázatmenedzsment, becslésének, elemzésének, értékelésének és kezelésének módszerei;
- 6. Az üzletmenet-folytonosság és a katasztrófa-elhárítás tervezése (BCP/DRP) és működtetése;
- 7. A fizikai biztonság és az őrzés-védelem; A hagyományos, papír alapú információk védelme;
- Gyakorlat: kockázatkezelési terv

Informatikai Rendszerek Minőségbiztosítása és Auditja V. A kockázatmenedzsment

Győrffyné Holló Krisztina
PE informatikai biztonsági szakértő, ISMS lead auditor

A kockázatmenedzsment

A kockázatmenedzsment

Miért? Mire?

Előnyök:

- megelőzés
- szisztematikus
- átfogó
- egységes eredményt ad
- hatékonyság növelő

Szükséges feltételek:

- erőforrások (idő, pénz, kompetencia)

A folyamatos fejlesztés egyik alapvető eszköze.

A kockázatmenedzsment

Alapfogalmak

A **veszély**:

- károkozási potenciál
- a biztonság hiánya
- olyan tulajdonság vagy helyzet, amely bizonyos körülmények között kárt okozhat.

Mi a **kockázat**?

- A kockázat a veszély megnyilvánulásának gyakorisága (valószínűsége) és a káros következmény nagyságának kombinációja.

(Royal Society, 1992)

A kockázatmenedzsment

Alapfogalmak (ISO)

ISO Guide 73:2009

- Kockázat: A bizonytalanság hatása a célokra
- Kockázatmenedzsment: Összehangolt tevékenységek egy szervezet kockázati szempontú irányítására és ellenőrzésére
- Kockázatmenedzsment keretrendszere: A szervezeten belül a kockázatmenedzsment tervezésének, bevezetésének, megfigyelésének, átvizsgálásának és folyamatos fejlesztésének alapjai és szervezeti intézkedéseit jelentő intézkedések összessége.

www.iso.org

A kockázatmenedzsment

Elemzési technikák

- minden folyamat szabályozott legyen,
- legyen egyértelműen hozzárendelt felelőse
- folyamatok dokumentálása,
- egyértelmű a feladat meghatározása,
- későbbi visszakereshetőségi lehetőség

Kontroll	Megfelelőség (Igen/Nem)	Megjegyzés
A szervet informatikai biztonsági tisztségviselője vagy ezzel egyenértékű vezetői szintű hatóság ki van nevezve és felelős a információbiztonsági program végrehajtásáért és fenntartásáért, a hatékony programvégrehajtásért.		
Az információbiztonsági vezető csapatának vagy osztályának dedikált feladat és felelősség az információbiztonsági tevékenység folytatása a szervezetben, beleértve a biztonsági adminisztrációt, a tudatossági oktatást és tréninget, fejlesztést és esemény kivizsgálásokat.		

A kockázatmenedzsment

Kontrollok meghatározása

Információbiztonsági szabályzat	A felsővezetés irányultsága és támogatása az információbiztonsági program vonatkozásában egyértelműen megalapozott.	I……. N……..
Információbiztonsági szabályzat dokumentáció	Van-e a felsővezetés által jóváhagyott információbiztonsági program?	I……. N……..

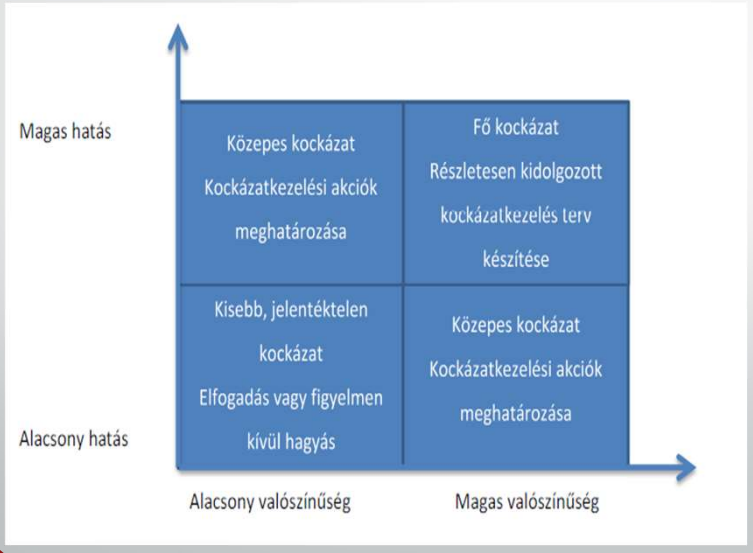
A kockázatmenedzsment

CRAMM – kockázatkezelési módszer

- CCTA Risk Analysis and Management Method, Egyesült Királyság (Central Computer and Telecommunications Agency)

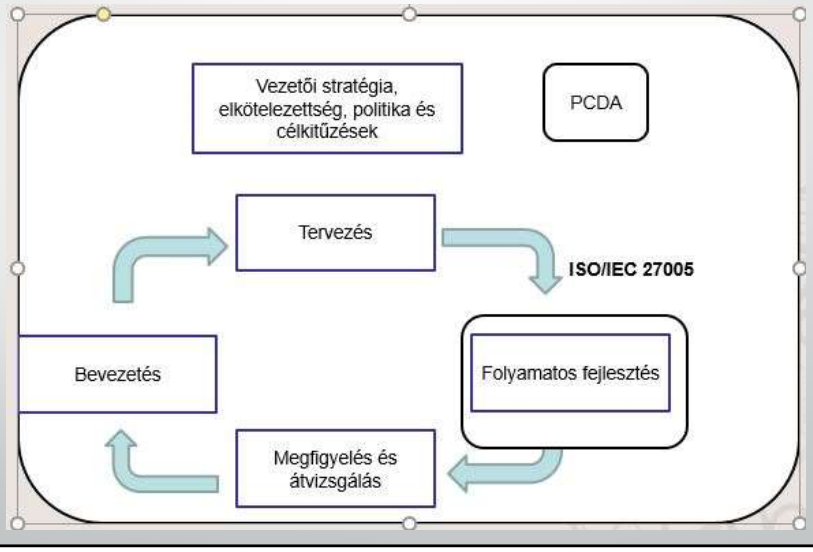
1. Védelmi igény feltárása (felmérés és értékelés)
2. Fenyegetettség elemzés
   - Fenyegetett rendszerelemek felmérése
   - Alapfenyegetettségek meghatározása
   - Fenyegető tényezők meghatározása
3. Kockázatelemzés
   - Fenyegetett rendszerelemek értékelése
   - Károk gyakoriságának meghatározása
   - Kockázat meghatározása
4. Kockázatkezelés
   - Intézkedések kiválasztása, értékelése
   - Költség/hasznon arány elemzése
   - Maradvány-kockázat elemzése

A kockázatmenedzsment



A kockázatmenedzsment

ISO/IEC 31000



A kockázatmenedzsment

Kockázatkezelési terv, alapelvek

- Értéket teremt és védi a szervezetet
- A szervezet folyamatainak szerves része
- Döntéshozatal segédeszköze, elősegíti a tényeken alapuló döntéshozatalt és kiküszöböli a bizonytalanságot
- Rendszeres, ismétlődő, strukturált és aktualitásokat tartalmaz
- Szubjektív, nem teljes körű, közelít az objektívhez
- Testreszabott
- Szervezeti, emberi és környezeti tényezők figyelembe vétele
- Könnyen áttekinthető, érintettek bevonásával készül
- Dinamikus, iteratív, érzékeny a változásokra
- Fejlődés elősegítő

A kockázatmenedzsment

Kockázatkezelési terv

- Általános követelmények:
- Az óvintézkedéseket az általános üzleti kockázatokkal összefüggésben kell bevezetni.
- A választott szabályozások visszavezethetők kell legyenek a
- a kockázatértékelésre,
- a kockázatjavítási eljárásra,
- az Információ biztonsági és irányítási rendszer (ISMS) politikájára és
- az ISMS-ben meghatározott célokra (4.3.1)

A kockázatmenedzsment

Kockázatkezelési terv (RMP)

Kockázatfelmérési környezet (context)

MSZ ISO/IEC 27001:2015 és ISO Guide 73:2009

Meg kell határozni

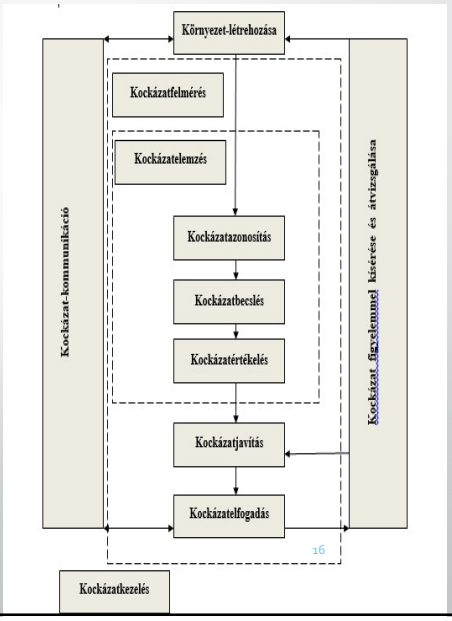
- az ISMS alkalmazási területét (Scope),
- az ISMS politikát,
- a kockázatfelmérés módját, és
- azonosítani kell a bizalmasság, sértetlenség, rendelkezésre állás elvesztésének/ sérülésének hatásait,
- ki kell alakítani a kockázatok elfogadásának kritériumrendszerét és a kockázat elfogadhatósági szinteket.

A kockázatmenedzsment

Kockázatkezelési terv részei

Kockázatfelmérési terv:

- Kockázatelemzés
- Kockázatbecslés
- Kockázatértékelés



A kockázatmenedzsment

Kockázatelemzés (analysis)
MSZ ISO/IEC 27001:2015 és ISO Guide 73:2009

Azonosítani kell:

- a **vagyonelemeket**
- a **fenyegetéseket**
- a **sérülékenységeket**
- a bizalmasság, sértetlenség, rendelkezésre állás elvesztésének/ sérülésének **hatásait**
- azokat az **eseményeket**, amelyek az üzleti folyamatot megszakíthatják.

Az informatikai kockázatelemzés nem védelmi intézkedés, elvégzése önmagában nem erősíti a védelmet, de segítség lehet ahhoz, hogy létrejöhessen egy biztonságos informatikai rendszer.

17

A kockázatmenedzsment

Kockázatelemzés (analysis)

- működési hatás elemzés,
- vagyonelemek kategorizálása,
- vagyonelemek értékelése: fenyegetések, sebezhetőségek szempontjából,
- veszély hatásának mértéke és skálája,
- támogató folyamatok kritikussága, osztályozása,
- kockázatkezelés határértéke.

Feladat:

- **Helyzetfelmérés, fenyegetettség, sérülékenység vizsgálat**
- **Módszertan kiválasztása (*CRAMM*, Gap, ITB, COBIT)**

18

A kockázatmenedzsment

Kockázatelemzés (analysis)

Használható segédeszközök:

- Tananyag feladatai
- neih.gov.hu (táblázatok)
- 2013. évi L tv. az állami és önkormányzati szervek elektronikus információbiztonságáról
- 41/2015. BM rendelet (…biztonsági osztály és biztonsági szintbe sorolására vonatkozó követelményekről)

Szükséges eszközök:

- Papír, toll, szabályozási és módszertani ismeretek, gondolkodás… ☺

A kockázatmenedzsment

Kockázatelemzés (analysis)

Vagyontárgyak azonosítása

Elsődleges/ másodlagos vagyonelemek csoportok:

- Szerződés alapú „üzleti" folyamatok és tevékenységek
  - (Informatikai belső hálózat (internet szolgáltatás), Tanulmányi/ gazdasági rendszer szolgáltatása, Honlap szolgáltatás, Iktató- és dokumentumkezelő-rendszer szolgáltatása, Video-streaming, VoIP, Telefonszolgáltatás, Riasztórendszer, Levelezőrendszer szolgáltatás, Központi fájlkezelés, Levelezőlisták szolgáltatása, Biztonsági adatmentés rendszerének szolgáltatása: elektronikus dokumentumok, központi rendszerek…, Helpdesk/ügyfélkiszolgálás)
- Információ típusok pl:
  - Elektronikus vagy papír alapú
  - személyes / üzleti / közérdekű adatok
  - nyílt / bizalmas vagy alap / normál / kritikus
- Tárolás helye szerint
- Eszközök: hardver, szoftver, hálózat, munkavállalók, szolgáltatások

A kockázatmenedzsment

Kockázatelemzés (analysis)

Fenyegetések azonosítása

Veszélyforrás: nem várt esemény bekövetkeztének lehetősége, ami a szervezet eszközeinek sérülését eredményezheti.

A fenyegetés típusa

- fizikai rongálás: tűz, víz, környezetszennyezés
- természeti jelenségek:
  - hidrológiai (árvíz, havazás)
- klimatikus/légköri
  - éghajlati (túlmelegedés, szélvihar, klímaváltozás)
  - légköri (villám)
- geológiai:
  - szeizmikus (földrengés)
  - vulkanikus (valószínűsége csekély)
  - földcsuszamlás (valószínűsége csekély)
  - a Föld mágneses terének gyengülése
- tűz által okozott katasztrófák

21

A kockázatmenedzsment

Kockázatelemzés (analysis)

Fenyegetések azonosítása

A fenyegetés típusa

- Alapvető szolgáltatás kimaradás okozta veszteség (Loss of essential services)
  - elektromos áram (áramszünet)
  - túlterhelés
  - légkondicionálás (légkondicionáló leállása)
  - távközlés (szolgáltatás kimaradás)
  - hálózati szolgáltatás (kimaradása)
- Ember, informatikai technika által okozott
  - Admin

  System Administrator

  Leírás: rendszeralkalmazás telepítése, üzemeltetése, karbantartása és cseréje. Jó szándékú vagy ellenséges ügyintézők: alkalmazás rendszergazdák vagy rendszeradminisztrátorok.

22

A kockázatmenedzsment

Kockázatelemzés (analysis)

Fenyegetések azonosítása

A fenyegetés típusa

- Ember, informatikai technika által okozott, szándékos vagy véletlenszerű fenyegetés
- Admin
  - biztonsági, adminisztrációs hiba
  - mulasztási, adminisztrációs hiba
  - rosszindulatú rendszergazdai vagy rendszerfelhasználói - adatok módosítása
  - a rendszeradminisztrátor megsérti az adatvédelmi politikát
  - rosszindulatú kódkihasználás
  - hamis rendszerszolgáltatás

23

A kockázatmenedzsment

Kockázatelemzés (analysis)

Fenyegetések azonosítása

- Ember, informatikai technika által okozott, szándékos vagy véletlenszerű fenyegetés
- Hacker - Rosszindulatú, illetéktelen személy

Leírás: általában egy külső, jogosulatlan felhasználó, aki illetéktelenül próbál az adott rendszerhez hozzáférni.

- Hacker hálózati hozzáférése
- erőforrások megszerzéséhez irányuló próbálkozásai
- beavatkozása a felhasználói adatátvitel során
- Kriptoanalízis
- IP-maszkolás
- üzenet tartalmának módosítása
- Hacker fizikai környezethez való hozzáférése
- „social engineering", megtévesztés
- rosszindulatú kód kihasználása (malware)
- hamis rendszerszolgáltatás (spoofing) stb.

24

https://hetpecset.hu/site/articles/view/harommillio-androidos-kartevo-2017-ben

A kockázatmenedzsment

Kockázatelemzés (analysis)

Fenyegetések azonosítása

- Ember, informatikai technika által okozott, szándékos vagy véletlenszerű fenyegetés
- Fizikai környezet fenyegetése

  Leírás: Az informatikai eszköz minden olyan sérülése, amelyet természeti katasztrófa vagy egyéb, nem emberi beavatkozás, okoz. Ez magában foglalja a hőt, a kozmikus sugarakat és egyéb tényezőket, amelyek hozzájárulnak a hardveröregedéshez.
- Rendszerbiztonságot fenyegető veszélyek
- Rendszer/hardver/szoftver

  Leírás: A fenyegetések szorosan köthetők rendszerhibához, de egy rendszerhiba is eredményezhet hardver- vagy szoftver hibát. Például: vírussal fertőzött a levelezőszerver.

25

A kockázatmenedzsment

Kockázatelemzés (analysis)

Fenyegetések azonosítása

- Ember, informatikai technika által okozott, szándékos vagy véletlenszerű fenyegetés
- Jogosult felhasználó (user)

  Leírás: A felhasználó jogosultsággal történő visszaélése.
  - titkosság megsértésére irányuló felhasználói cselekmények
  - adatgyűjtés
  - olyan cselekedet, amellyel elérhetetlenné teszi az adatokat
  - integritási hiba
  - rendszer biztonsági funkcióinak megsértése
  - szolgáltatás-megtagadás
  - nem engedélyezett adatmódosítás
  - nem engedélyezett adatküldés
  - nem engedélyezett adatkezelés stb.

26

A kockázatmenedzsment

Kockázatelemzés (analysis)

Fenyegetések azonosítása

- Eredet szerint:
- Szándékos: célja a tájékoztatás eszköz
  - kémkedés
  - illegális adatok feldolgozása
- Véletlen
  - berendezés meghibásodása
  - szoftver hiba
- Környezeti
  - természeti esemény
  - áramkimaradás esetén
- Gondatlanságból: Ismert, de elhanyagolt tényezők, amely veszélyezteti a hálózati biztonságot és a fenntarthatóságot.

27

A kockázatmenedzsment

Kockázatelemzés (analysis)

Meglévő intézkedések azonosítása

- Szabályozás
- Tényeken alapuló döntéshozatal
- Bizonyítékok: dokumentáció, eredmények.

Sebezhetőségek azonosítása:

- Sérülékenységek
- Gyengeségek és hiányosságok

A sebezhetőség önmagában nem okoz kárt, de lehetővé teszi a fenyegetések aktiválását. Kezelése szükséges.

(nem megfelelő felhasználói jogosultságok, kábelrengeteg, bezáratlan ajtó)

28

A kockázatmenedzsment

Kockázatelemzés (analysis)

Következmények azonosítása (ok-okozati tényezők felállítása)

Incidens által okozható kár, egyéb következmény

- Azonnali – jövőbeni bekövetkezés

(áramszünet – adatvesztés, hibás programozás – hibás adatösszegzés)

- Közvetlen – közvetett módon hat
- Ideiglenes – maradandó

(adatvesztés – helyreállítás, eszközök elöregedése - storage meghibásodás, szerverszoba hőmérséklet emelkedés – hardver eszközök meghibásodása)

29

A kockázatmenedzsment

Kockázatbecslés (estimation)

ISO/IEC 27001:2013 és ISO Guide 73:2009

Módszerek:

- Kvalitatív (sorrendezés)
- Fél-kvantitatív (numerikus skála, érték nélkül)
- Kvantitatív (numerikus skála értékkel)

A vagyonelem csoportonként eltérő mélységű lehet.

30

A kockázatmenedzsment

Kockázatjavítás (treatment)

ISO/IEC 27001:2013 és ISO Guide 73:2009

- Intézkedések kiválasztása
- Kockázatjavítás életciklusa
  - Kockázatjavítási terv
  - Maradvány kockázat
  - Kockázatelfogadás

31

A kockázatmenedzsment

Kockázatjavítás (treatment)

ISO/IEC 27001:2013 és ISO Guide 73:2009

- Intézkedések kiválasztása
- Intézkedések kiválasztásának és bevezetésének folyamata a kockázatkezelés, -elfogadási szint és a –javítás függvényében.
- Intézkedések bevezetése:
  - Költség-haszon elemzés, arányosság
  - Egyidejűleg több intézkedés is bevezethető
  - Új kockázatokat hozhat létre
  - Több kockázatot módosíthat

32

A kockázatmenedzsment

Intézkedések osztályozása - adminisztratív

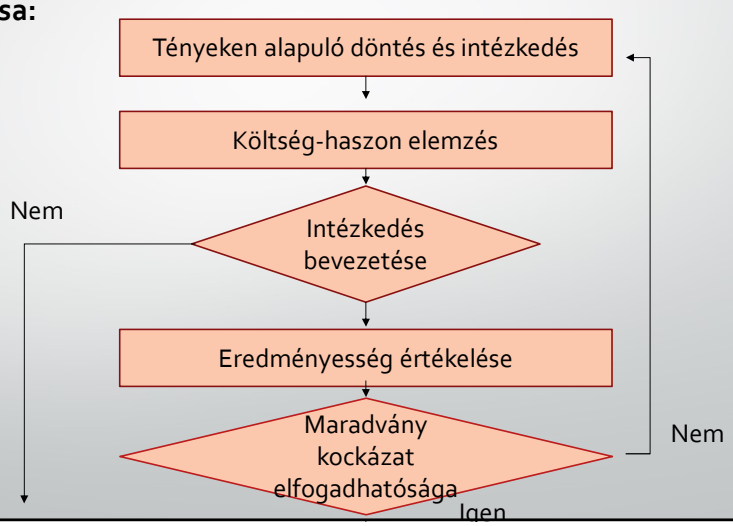
- Szabályzatok
- Szokások/ gyakorlat
- Eljárások
- Szervezeti struktúra (outsource, adatrögítő, jóváhagyó)
- Szoftver, hardver megoldások
- Fizikai védelem

- Megelőző
- Észlelő
- Elhárító

33

A kockázatmenedzsment

Kockázatjavítás ciklusa:



34

A kockázatmenedzsment

Kockázatjavítási terv

- Kiválasztott intézkedések
- Határidők
- Felelősök

- Kiválasztás oka – indoklás, lehetséges haszon
- Prioritások kezelése
- Szükséges költségek, erőforrások becslése
- Teljesítmény mérés módja (módszer kiválasztás, tesztelés)
- Jelentési és megfigyelési dokumentációk – követelmények alapján

35

A kockázatmenedzsment

Maradványkockázat

- Intézkedések bevezetése
- Elemzés
- Maradványkockázat megállapítása, értékelése
- Óvintézkedések bevezetése

Teljes kockázatmentesség nem létezik!

36

A kockázatmenedzsment

Kockázat elfogadása (acceptance)

- Elemzés – tények – döntés
- Megalapozott döntés egy meghatározott kockázat elfogadásáról (tényeken alapuló döntéshozatal)
- Kockázatjavítás után vagy nélküle

37

A kockázatmenedzsment

Kockázatok figyelemmel kísérése és átvizsgálása

- Óvintézkedések hatásosak (szabvány) és hatékonyak (A melléklet)
- Információgyűjtés a kockázatfelmérés javítására
- Események, változások, trendek, sikerek és kudarcok elemzése, tanulságok levonása
- Változások észlelése a külső és belső környezetben
- Új kockázatok azonosítása (fenyegetések megváltozása, új kockázatok jelennek meg
- Monitoring rendszer használata: belső audit, statisztikai adatok, eredményességi mutatók, vezetőségi átvizsgálás, külső audit (lehetőség szerint) = figyelemmel kísérés

38

A kockázatmenedzsment

Kommunikáció

- A kockázatokkal kapcsolatos információk cseréje illetve megosztása a döntéshozó és más érintett felek között (ISO/IEC Guide 73:2002)
- A szervezet által végrehajtott folyamatos és iteratív folyamat a kockázatmenedzsmenttel kapcsolatos információk átadására, megosztására és megszerzésére, valamint az érintett felekkel való párbeszéd fenntartására (ISO/IEC Guide 73:2009)

39

A kockázatmenedzsment

Kommunikáció

- Belső és külső érintett felek
- Kommunikációs és konzultációs terv
- Felelősök kijelölése
  - Vezetői képességek, taktika, tárgyalási- és kommunikációs ismeretek
- Bizalmasság (titoktartás, személyes érdekek)
- Konzultációs csoport előnyei
  - Környezet megfelelő azonosítása
  - Különböző szakterületek véleményének figyelembe vétele
  - Széleskörű belső támogatás
  - Hatékony változáskezelés

40

Informatikai Rendszerek Minőségbiztosítása és Auditja VI. Az üzletmenet-folytonosság BCP/DRP

Győrffyné Holló Krisztina

PE informatikai biztonsági szakértő, ISMS lead auditor

BCP/DRP

Informatikai üzletmenet-folytonossági terv

Informatikai katasztrófa-elhárítási terv

Előnyök:

- az informatikai szolgáltatás folyamatosságának biztosítása,
- a támogatott és működtetett informatikai folyamatokat, rendszereket és alkalmazásokat ért katasztrófa utáni gyors, rendezett és megfelelő (gyártó által támogatott) helyreállítási tevékenység végrehajtása, felhasználói megelégedettség elnyerése,
- informatikai fejlesztési tervek biztosabb teljesítése,
- informatikai hatékonyságnövelés,
- megalapozott döntéshozatal,
- kedvezőtlen események elkerülése,
- bizalmasság, sértetlenség, rendelkezésre állás teljesíthetősége.

BCP

Informatikai üzletmenet-folytonossági terv

Előnyök:

- egyes kritikus működési folyamatokhoz tartozó támogató vagy
- alternatív folyamatok megadása.

Pl.:
Ha az adott alternatív folyamat csak **alacsony mértékben** támogatja (kis mértékben helyettesíti) a fő folyamatot, akkor ezt a tényt **„1"-es** osztályzattal értékeljük.
Vagy
Ha az adott alternatív folyamat **teljes körűen** támogatja (azaz ténylegesen helyettesíti) a fő folyamatot, akkor ezt a tényt **„4"-as** osztályzattal értékeljük.

BCP

Informatikai üzletmenet-folytonossági terv

A lehetséges tesztelési módok:

- strukturált „végigsétálás - walk-through"
- ellenőrző kérdésjegyzék (check-list) alapú teszt
- szimuláció
- párhuzamos tesztelés
- teljes megszakításos teszt

DRP

Informatikai katasztrófa-elhárítási terv

- A DRP **célja**, hogy az adott szervezet információs rendszerében a kritikus szolgáltatások folyamatos működésének biztosítása az üzleti követelményeknek megfelelően,
  - az informatikai katasztrófa bekövetkezte esetén fellépő kár csökkentése,
  - a szükséges szolgáltatások elérhetővé tétele és folyamatosságának biztosítása,
  - a rendeltetésszerű működés visszaállításának felgyorsítása egy rendszeresen karbantartható, strukturált
- informatikai katasztrófa-elhárítási tervalapján.

DRP

Informatikai katasztrófa-elhárítási terv

- Katasztrófa az informatikai rendszerben minden olyan esemény, ami a Szervezet üzleti tevékenységének folyamatosságát az informatikai rendszer kritikus szolgáltatásait, sebezhetőségét nagy mértékben meghaladó kieséssel sérti vagy fenyegeti. (sebezhetőségi ablak)
- Ilyen eseményt előidézhet, de nem kizárólagosan:
  - az elemi kár: tűzvész, villámcsapás, robbanás vagy más külső behatás,
  - a Szervezet fő folyamatait befolyásoló elektromos hálózat tartós kiesése,
  - a telekommunikációs hálózat tartós kiesése (riasztó),
  - kritikus informatikai rendszerek súlyos üzemzavara.
- Lényeges, hogy az adott konkrét helyzetet sohasem a kiváltó ok, hanem mindig a kiváltott okozat alapján lehet és kell megítélni.

DRP

Informatikai katasztrófa-elhárítási terv

A katasztrófa menedzser
- irányítja az informatikai katasztrófa elhárítását.

Ennek keretében:
- a rendelkezésére álló információk alapján kinyilvánítja az informatikai katasztrófa állapotot,
- informatikai katasztrófa helyzetben dönt a szakértők és / vagy harmadik fél, különösen a tűzoltók, mentők hívásáról,
- a rendelkezésére álló információk alapján dönt a normál üzemre való visszaállásról,
- kezdeményezheti a DRP kiegészítő terve végrehajtásának megkezdését.

DRP

Informatikai katasztrófa-elhárítási terv

A szakértők:
- informatikai katasztrófa helyzetben az élet és vagyonbiztonságot közvetlenül fenyegető veszélyek elhárításában utasításra vagy egyes esetekben öntevékenyen vesznek részt,
- képzettségüknek megfelelően közreműködnek a váratlan események következményeinek feltárásában,
- ellenőrzik a hozzájuk tartozó erőforrások épségét, tesztelik a berendezéseket,
- rendszeresen tájékoztatják a vezetőt (krízist koordinátor),
- képzettségüknek megfelelően közreműködnek a szolgáltatások eredeti vagy csökkentett funkcióinak helyreállításában.

DRP

Informatikai katasztrófa-elhárítási terv

Általános előírások:

- Elsősegély: elsődleges feladat a személyzet életének és testi épségének védelme. Minden egyéb feladat csak akkor kezdhető meg, ha a veszélyeztetett személyek biztonságba kerültek.
- Biztonsági követelmények
- Szükséges biztonsági folyamatok és felelősök meghatározása
- Események naplózása
- Teendők informatikai katasztrófa esetén (A DRP aktiválása, átfogó akcióterv, események behatárolása - teendők, elhárítási csoport megnevezése, összehívása, érintett felek értesítése, áttelepülés a központi tartalék munkahelyekre)
- Készenléti állapot meghatározása
- Kiegészítő terv

Informatikai Rendszerek Minőségbiztosítása és Auditja
VII. A fizikai biztonság és az őrzés-védelem A hagyományos, papír alapú információk védelme

Győrffyné Holló Krisztina

PE informatikai biztonsági szakértő, ISMS lead auditor

A fizikai biztonság és az őrzés-védelem

Helyzetfelmérés

A **fizikai biztonság**gal kapcsolatban léteznek-e védelmi intézkedések:

- a hardver eszközök,
- a berendezések,
- a központi számítógép és
- a gépterem fizikai meghibásodásának, károsodásának kiküszöbölésére (hidegtartalék eszközök, stb.);
  - a számítógépekhez,
  - a gépteremhez,
  - az egyéb eszközökhöz való hozzáférések korlátozására (zárt helyiségek, BIOS jelszó, billentyűzetzárolás, stb.);
    - a jogosult hozzáférések regisztrálására,
    - naplózására.

A fizikai biztonság és az őrzés-védelem

Helyzetfelmérés

A **logikai biztonság**gal kapcsolatban léteznek-e védelmi intézkedések

- a felhasználók azonosítására, hitelesítésére, valamint
- a bejelentkezések ellenőrzésére,
- a jelszavak, kulcsszavak kiadására, használatára, visszavonására és nyilvántartására;
- a nem aktív felhasználók kiszűrésére;
- a speciális jogosultságokkal, privilégiumokkal rendelkezők hozzáféréseinek nyomon követésére,
- a sikertelen bejelentkezések figyelésére, naplózására;
- a hozzáférés-biztonsági és jogosultsági rendszer kiterjed-e az alkalmazások, adat- és program-állományok, adatbázisok, tranzakciók kezelésének engedélyezésére, szabályozásának kialakítására és betartásuk ellenőrzésére.

A fizikai biztonság és az őrzés-védelem

Helyzetfelmérés

A **fenyegetettség és sebezhetőség elemzés** végrehajtását követően **aktualizálnia kell**:

- az informatikai infrastruktúrájának aktualizált logikai leírását;
- az informatikai infrastruktúrájának aktualizált fizikai leírását;
- a hálózat felépítését leíró dokumentációt;
- az érintett rendszerelemek listáját;
- az vagyonelemek és rendszerelemek függőségi mátrixát;
- az informatikai erőforrások sebezhetőségeinek listáját;

A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

- Objektum (befogadó épület) és a gépterem épületgépészete
- Behatolás elleni védelem
- Beléptető rendszer (porta, kártyás, videó) felügyelettel
- Légkondicionálás
- Tűzvédelem
- Tűzbiztos adathordozói védelem
- Folyamatos áramellátás (generátor, szünetmentes)
- Sugárvédelem, vezetett zavarvédelem
- Túláram és túlfeszültség-védelem
- Elektrosztatikus védelem
- Rezgésvédelem és csillapítás
- Üzletmenet-folytonosság és katasztrófa-elhárítás

A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Felmerülő problémák:

- Inhomogén rendszerek (beléptető-, videorendszerek)
- „Szigetek”
- Komplex biztonsági felfogás hiánya
- Meglévő rendszerek tudásának kihasználatlansága
- Nagy mennyiségű és nagy méretű napló állományok felhasználatlansága
- Manuális beavatkozások
- Automatikus incidenskezelés vagy eseménykezelés hiánya

A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Elhelyezési szempontok:

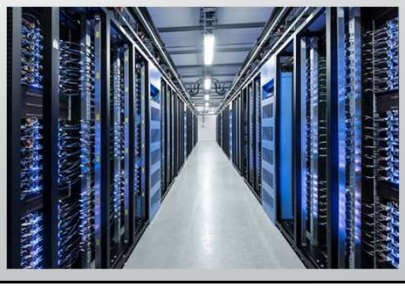
- Emeleti és földfelszín alatti elhelyezés előnyei – hátrányai
- Szabályozott és kontrollált megközelíthetőség
- Erős „héj” védelem
- Közlekedési útvonalak, nyílászárók, liftek
- Környező belső épületfunkciók
- „Nedves” infrastruktúra
- Erősáramú zavarforrások

A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Elhelyezési szempontok:

- Elhelyezkedés: egy belső épületben lehetőleg földszint alatt
- Figyelembe kell venni:
- a lehetséges fizikai behatolási pontokat,
- a természetes illetve mesterséges vizek elleni védekezést,
- a kinti forgalom - rezgést,
- az elektromágneses
- sugárzás elleni árnyékolást



A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Egyes esetekben robbanóanyagok, vegyi anyagok elleni védelemről is intézkedni kell.

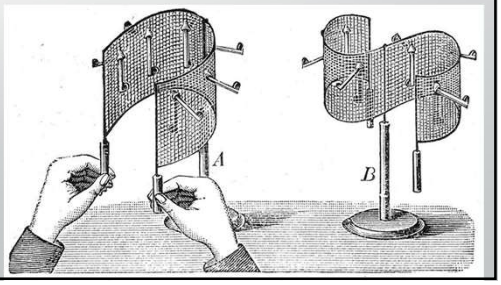
A cél: az objektum körkörös védhetősége

megfelelő héjvédelem és kültéri védelem

Az elektromágneses sugárzás elleni védelem:

felszíni épületrészeknél Faraday kalitkával

földszint alatti épületrészeknél vasbeton szerkezet



A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Erőforrás – villamos energia:

- legfontosabb erőforrás
- szükségellátásról több szinten kell gondoskodni
- épület szintű betáplálás:
  - lehetőleg két, egymástól független alállomásról történjen,
  - megfelelő védelemmel ellátva.
- az energiaellátás folyamatos biztosítása érdekében:
  - szünetmentes áramforrások alkalmazása, (rövidtávú kimaradásokra)
  - dízelgenerátorok (hosszabb távra)

A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Környezeti jellemzők megfelelő szinten tartása:

- léghőmérséklet és páratartalom
  - légkondicionáló berendezésekkel tartható megfelelő szinten
  - redundáns kialakítás (teljes értékű) és
  - helyettesíthetőség figyelembe vétele:
    - lehetőleg párosával kerüljenek elhelyezésre,
    - szomszédos berendezés elláthatja a kiesett egység feladatát.

Hosszú távú adattárolás - a levegő nedvességtartalmának a szoros kapcsolata (papír és elektronikus adattárolás)

A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Tűzvédelem

- *szigorúbb előírások*: a minél gyorsabb oltás és a legkisebb anyagi kár elérésére.
- érzékelés szempontjából:
  - aspirációs *füstérzékelők* telepítése:
    - gyorsabban és nagyobb biztonsággal érzékeli a keletkező tüzet.
    - a szerverterembe telepített több szívócsonkból, központi légbeszívásból és egy analizáló berendezésből áll.
    - de rendkívül költséges,
  - pontszerű optikai füstérzékelés továbbra is elterjedtebb.
  - *automatikus oltórendszer* alkalmazás (alapvető követelmény) – manuális oltó berendezéssel kombinálva

A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Tűzvédelem

- oltás:
  - *inert gáz* alkalmazásával, vagy
  - *vízköddel* oltó berendezéssel - nem bizonyult megfelelőnek, komoly anyagi károkat okozott

(a szerverteremben lévő szálló por

a vízködöt vezetővé teszi)

A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Vagyonvédelem:

- hagyományos objektumvédelmi feladatokhoz hasonló, de nagyobb a jelentősége
- védett körletek kialakítása
- *belépési jogosultság*

szerepkörök alapján

történő kialakítása

A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Vagyonvédelem, alapvető követelmény:

- központi jogosultságkezelés kétfaktoros azonosítással, (proximity kártyás és PIN kódos)
- jogok kiosztása központi rendszerben,
- együttes vezetői jóváhagyás
- rendszeres jogosultság felülvizsgálat: legalább évente (automatikus vagy manuális összehasonlítás)
- eltérések kivizsgálása
- belépések naplózása (pl. ha három napig lehet tárolni, ezen időszakon belüli, illegális behatolások, vagy jogosultság-túllépések felderítése) - hatályos adatvédelmi szabályozások szerint

A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Bizonyítékok tárolása

- tárolás idejének meghosszabbítása: a rendőrségi feljelentés vagy a fegyelmi eljárás lefolytatásáig.

A biztonsági körletek követelményei:

- szervezeti egységek területeinek fizikai elválasztása
- (a karbantartók, a logisztika, az informatikai részektől)
- szerverpark több teremben kerüljön elhelyezésre funkcionális illetve biztonsági szempontok alapján
- védett körletek kamerás megfigyelése, (átjárók és a munkavégzés területei), három napos megőrzési határidő

A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Ablakok, ajtók:

- lehetőleg ne rendelkezzenek ablakokkal illetve nem védett térbe nyíló ajtókkal. (biztonsági rácsok, üvegtörés érzékelő és a védett oldalra telepített passzív infravörös érzékelők alkalmazásával)

Az ajtók:

- biztonsági okokból legyenek - zsilip rendszerűek, életvédelmi okból - a szerverterem felőli ajtó kilinccsel nyitható, vagy vésznyitó kulcs az ajtó mellett. (menekülés biztosítása)
- életvédelmi okból szintén szükséges az oltógáz indítását blokkoló nyomógomb elhelyezése a védett helyiségen belül.

A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Az informatikai rendszer védelme

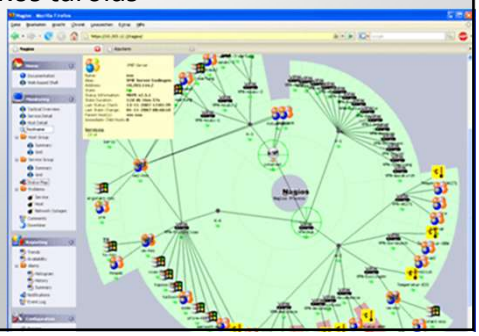
- Tűzfal - minden külső forgalomnak kötelező (titkosított protokollok pl. HTTPS, SFTP, SSH)
- A szervertermen belüli forgalom lehet titkosítás nélküli.
- A szerverekre való belépés
- személyre kiosztott, és
- több vezetői szinten engedélyezett hozzáféréssel
- Naplózás – naplószerver (meghatározott hozzáféréssel)
- sikertelen és sikeres belépések, valamint
- különösen védendő rendszerek esetén minden tevékenységet

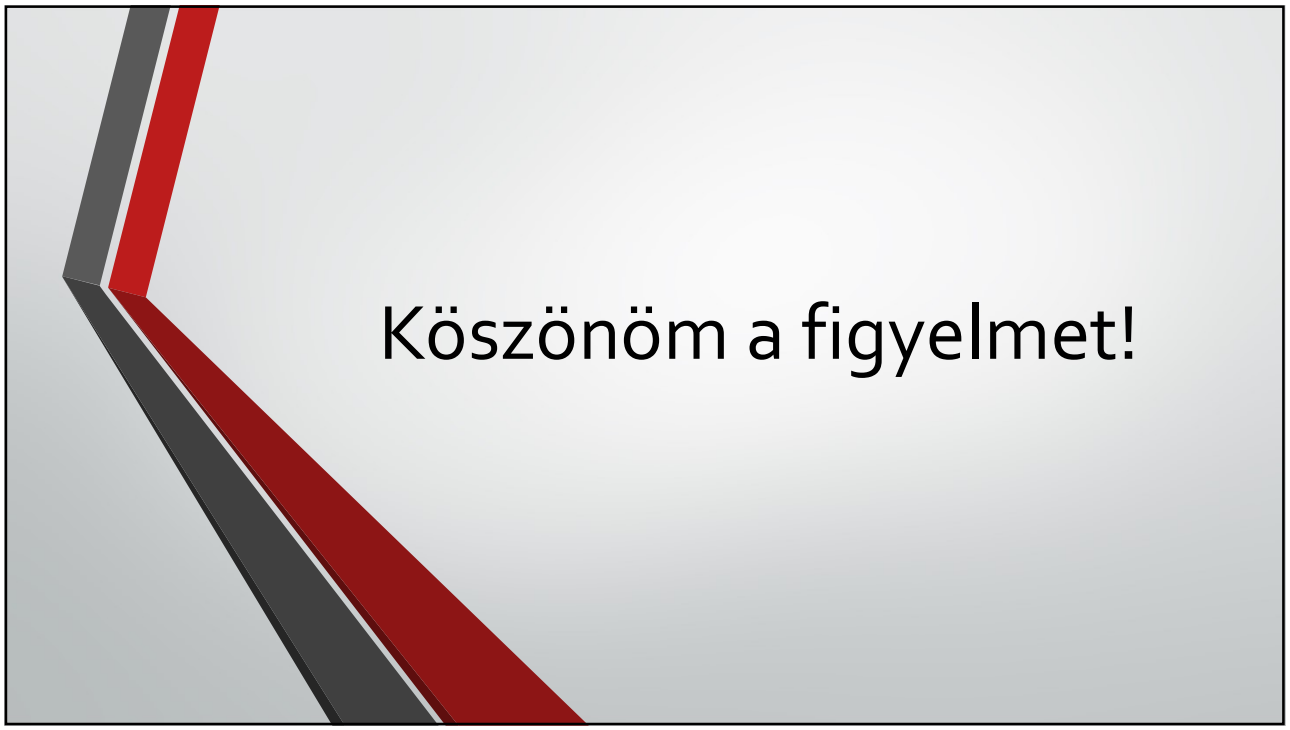
A fizikai biztonság és az őrzés-védelem

A fizikai biztonság legfontosabb kategóriái – épülettervezés, számítógépterem

Naplószerver (meghatározott hozzáféréssel)

- Bizonyíték
- Mentés – fizikai tárolás – titkosított elektronikus tárolás
- Biztonsági eljárások – előírások




Köszönöm a figyelmet!

Informatikai Rendszerek Minőségbiztosítása és Auditja IV.

Győrffyné Holló Krisztina
PE informatikai biztonsági szakértő, ISMS lead auditor
2021.10.08.

Témák

- 8. A személyek, emberi erőforrás védelme (infotv és GDPR); Az informatikai védelem;
- 9. Katasztrófa-elhárítás információbiztonsági vonatkozási; Incidenskezelés;
- 10. Az információbiztonság működésének ellenőrzése, mérése;
- Gyakorlat: Intézkedési terv

Informatikai Rendszerek Minőségbiztosítása és Auditja
VIII. A személyek, emberi erőforrás védelme (infotv és GDPR)
Az informatikai védelem

Győrffyné Holló Krisztina

PE informatikai biztonsági szakértő, ISMS lead auditor

Az emberi erőforrás védelme

Alapvető fogalmak:

Személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

különleges adat:

a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat,

Az emberi erőforrás védelme

Alapvető fogalmak:

bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

Az emberi erőforrás védelme

Személyes adatok

Minden azonosított vagy azonosítható természetes személyre vonatkozó információ, akár az álnevesített személyes adatok is, amelyekről észszerűen feltételezhető, hogy az adatkezelő vagy más személy a természetes személy közvetlen vagy közvetett azonosítására felhasználhatja.

A természetes személyek összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel és cookie-azonosítókkal, egyéb azonosítókkal (rádiófrekvenciás azonosító címkék).

Ezáltal olyan **nyomok** keletkezhetnek, amelyek egyedi azonosítókkal és a szerverek által fogadott egyéb információkkal összekapcsolva felhasználhatók a **természetes személyes profiljának** létrehozására és az adott személy azonosítására.

Az emberi erőforrás védelme

Adatkezelés és feltételei

Az érintett egyértelmű előzetes nyilatkozatával, ami lehet:

- írásbeli (egyértelmű elektronikus úton tett is), vagy
- szóbeli,
- önkéntes, konkrét, előzetes tájékoztatáson alapuló és egyértelmű hozzájárulását adja a természetes személyt érintő személyes adatok kezeléséhez.

(A hallgatás vagy a nem cselekvés nem minősül hozzájárulásnak.)

Az emberi erőforrás védelme

Az adatkezelés

legyen

- jogszerű és korrekt,
- átlátható (tájékoztatás és a kommunikáció),
- a cél egyértelmű, jogszerű és az érintett szempontjából elfogadható,
- az adatkezelés, tárolás a lehető legrövidebb időre korlátozódjon,
- a törlés és az időszakos felülvizsgálat biztosított,
- az információk védelme (fizikai, logikai, adminisztratív) biztosított az illetéktelen hozzáféréstől.

Az emberi erőforrás védelme

Adatvédelmi hatásvizsgálat

- A természetes személyek jogaira és szabadságaira nézve magas kockázattal járó esetekben,
- új technológiák alkalmazása esetén, az érintettek adatainak védelme veszélyben lehet,
- kockázatos adatkezelés esetén (különleges adatok, technológiai jellegű adatok), tömeges megfigyelés (közterületi kamerákon keresztül).
- Az adatkezelés jellegét, hatókörét, körülményeit és céljait, a kockázat forrásait figyelembe véve kell felmérni a magas kockázat különös valószínűségét és súlyosságát.
- A hatásvizsgálat tartalma lehet:
  - kockázat mérséklése (kockázatkezelés),
  - a személyes adatok védelme (megoldások),
  - tervezett intézkedési tervek.

Az emberi erőforrás védelme

Adatvédelmi incidens

Adatvédelmi incidens fizikai, vagyoni és nem vagyoni károkat okozhat a természetes személynek.

- Fejleszteni kell a belső információs és védelmi rendszereket.
- Az adatvédelmi incidenseket 72 órán belül jelenteni kell a Hatóság felé (NAIH).
- Az incidensekről az érintetteket tájékoztatni kell.

Az emberi erőforrás védelme

Adatbiztonság

Az adatkezelő intézkedéseket hajt végre, a következő műveletekre:

- a személyes adatok anonimizálása (maszkolás) vagy titkosítása;
- a kezelésre használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítása, integritása, rendelkezésre állása és ellenálló képessége;
- fizikai vagy műszaki incidens esetén a hozzáférés és az adatok rendelkezésre állásának kellő időben való visszaállíthatósága;
- az adatkezelés biztonságának garantálása (technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárás).

Az emberi erőforrás védelme

Adatvédelem

Biztonságos hálózat és IT rendszer: hálózati védelem, tűzfal,

Adatok védelme:

- titkosítás,
- mobil eszközök titkosítása,
- adatátvitel titkosítása,
- helyreállítási képesség kialakítása, tesztek (mentés, BCP/DRP),

Sérülékenység kezelés:

- malware és vírusvédelem
- időszaki sérülékenység vizsgálatok, tesztek.

Az emberi erőforrás védelme

Adatvédelem

- Hozzáférés szabályozás és ellenőrzés
  - Azonosítás és hitelesítés szabályozás, ellenőrzése
  - Fizikai hozzáférések szabályozása, tesztek.
- Naplózás, monitoring
  - Monitoring rendszer,
  - Naplógyűjtő és logelemző rendszer,
- Személyi biztonság, képzések
  - Biztonsági szabályrendszerek kialakítása
  - Személyzet biztonságtudatossági oktatása

Az emberi erőforrás védelme

Érdekesség:

Android: https://hetpecset.hu/site/articles/view/millios-tomegek-kovetelik-a-vegleges-torlesuket-a-netrol

BKK: https://naih.hu/files/NAIH-2018-356-H_hatarozat.pdf

OMV: https://naih.hu/files/NAIH-2017-1961-H-hatarozat.pdf

Kamera használat: https://naih.hu/files/NAIH-2017-434-H_hatarozat.pdf

Informatikai Rendszerek Minőségbiztosítása és Auditja IX. Katasztrófa-elhárítás információbiztonsági vonatkozási Incidenskezelés

Győrffyné Holló Krisztina

PE informatikai biztonsági szakértő, ISMS lead auditor

DPR

Katasztrófa-elhárítás

- A DRP **célja,** hogy az adott szervezet információs rendszerében a kritikus szolgáltatások folyamatos működésének biztosítása az üzleti követelményeknek megfelelően,
  - az informatikai katasztrófa bekövetkezte esetén fellépő kár csökkentése,
  - a szükséges szolgáltatások elérhetővé tétele és folyamatosságának biztosítása,
  - a rendeltetésszerű működés visszaállításának felgyorsítása egy rendszeresen karbantartható, strukturált
- informatikai katasztrófa-elhárítási tervalapján.

További információ: 6. témakör Az üzletmenet-folytonosság és a katasztrófa-elhárítás tervezése (BCP/DRP) és működtetése (III. diasor)

Incidensek kezelése

- Irányelvek megfogalmazása (üzleti IB politika, a BCP és a RMP)
- irányelveket alkalmazza az információbiztonsági incidensek eljárásaira
- eljárások pl.:
  - információrendszer-hibák és a szolgáltatás elvesztésére,
  - rosszindulatú kód felderítésére,
  - a szolgáltatás megtagadására,
  - a nem teljes vagy nem pontos működési adatokból eredő hibák megoldására,
  - a bizalmasság és sértetlenség megsértésére,
  - az információrendszerekkel való visszaélésre vonatkozó előírások vagy megoldások.

Incidensek kezelése

Incidensek analizálása:

- az incidens okának elemzése, azonosítása és behatárolása,
- helyesbítő és megelőző tevékenységek, intézkedések,
- adatközlés érintettek részére,
- belső szervezeti problémaelemzés,
- szabályozás felülvizsgálata, intézkedések.

Informatikai Rendszerek Minőségbiztosítása és Auditja X. Az információbiztonság működésének ellenőrzése és mérése

Győrffyné Holló Krisztina

PE informatikai biztonsági szakértő, ISMS lead auditor

Az információbiztonság működésének ellenőrzése és mérése

Ellenőrzési és mérési eljárásokat kell kialakítania és működtetnie a szervezetnek:

- megfelel-e az előírásoknak (ISMS) meghatározott hatóköre,
- szükséges legyen újraértékelni a meghatározott feladatokat és felelősségeket,
- azonnal észlelni tudja a biztonsági eseményeket,
- a szervezet dolgozói a tevékenységeiket az elvárások (szabályzatok, eljárások) szerint hajtják-e végre,
- elősegítse a biztonsági események észlelését, -> megelőzhető a tényleges biztonsági esemény bekövetkezése, és csökkenthető az elszenvedhető kár mértéke,
- feltárhatóvá váljon a bevezetett védelmi intézkedések általi eredmények.
- az elkészített katasztrófa-elhárítási és üzletmenet-folytonossági tervek aktuálisak-e, biztosítják-e biztonsági esemény esetén az elvárt működést - tesztek.

Az információbiztonság működésének ellenőrzése és mérése

*Ellenőrzési és mérési eljárások*at kell kialakítania és működtetnie a szervezetnek:

- rendszeres kockázatfelmérési és elemzési felülvizsgálatok, maradványkockázatok és a meghatározott elfogadható, a szervezet számára elviselhető kockázati szintek vizsgálata során, figyelembe kell venni:
  - a szervezetben,
  - a technológiában,
  - a működési célokban és folyamatokban,
  - az azonosított fenyegetésekben,
  - a bevezetett intézkedések hatékonyságában és
  - a külső környezetben bekövetkezett változásokat.

Belső auditok

21

Az információbiztonság működésének ellenőrzése és mérése

Belső auditok

- Tervezés (folyamatok, területek, előző audit eredmények, sajátosságok)
- Auditálási folyamat: tárgyilagos, etikus, pártatlan

- Mérési eljárás kiválasztása, mérőrendszer kialakítása

A szervezet mérőrendszerét úgy kell kialakítania, hogy a mérések megismételhetőek legyenek, és a kapott eredmények összehasonlíthatósága biztosított legyen. A mérőrendszer kialakításának előfeltétele annak, hogy a szervezet meghatározza azokat célokat és mérési módszereket, melyekkel el tudja végezni a méréseit.

Ezek ismeretében már képes lesz mérni a folyamatait, tevékenységeinek hatékonyságát és hatásosságát.

Az információbiztonság működésének ellenőrzése és mérése

Területek, mérőszámok:

Informatikai mérések:

- Biztonsági események száma
- Rendszer rendelkezésre állási mérések
- Informatikai válaszidő mérése a megkeresésekre
- Meghibásodások számossága
- Felhasználói panaszok számossága

ISMS folyamatok működésének mérése:

- Korrekciós intézkedések száma
- Védelmi intézkedésekben meghatározott határidők betartása
- Védelmi intézkedések számossága
- Kritikus területek számossága
- Harmadik fél szolgáltatásainak igénybe vétele esetén az SLA szintek teljesítésének mérése
- Szabályok megsértésének számossága
- Biztonsági események számossága

Az információbiztonság működésének ellenőrzése és mérése

Az informatikai biztonság ellenőrzése, célja:
objektív információkat biztosításon a felelős vezetők számára az informatikai biztonság helyzetéről, amelyek alapján a kockázatok csökkenthetők, és a rendkívüli események elkerülhetővé válnak.

A vizsgálat kiterjedése:

- az informatikai rendszerek biztonsága megfelel-e a Szervezet által elfogadott biztonságpolitikának,
- érvényesülnek-e a jogszabályokban, a szervezeti és a rendszer szintű biztonságpolitikákban és szabályzatokban foglaltak,
- történnek-e az informatikai rendszerek, illetve az általuk nyújtott szolgáltatások biztonságát sértő események, illetve mekkora ezek bekövetkezési valószínűsége.

Hiányosságok feltárása, védelmi intézkedések, javítások.

Az információbiztonság működésének ellenőrzése és mérése

Az informatikai biztonsági ellenőrzések *formái*, típusai

(tárgyszerűség, valós helyzet feltárása)

- informatikai biztonsági vizsgálat (fenyegetettség, védelmi képesség elemzés kockázatelemzéssel),
- auditálás (meghatározott követelményeknek való megfelelés vizsgálata),
- informatikai biztonsági tanúsítás és minősítés (pl.: a Common Criteria, ISO 27001 követelményeinek való tanúsított megfelelés)

Az információbiztonság működésének ellenőrzése és mérése

Az ellenőrzés eszközei:

- személyes ellenőrzés,
- megfigyelés,
- információ bekérés,
- dokumentumok vizsgálata,
- technikai berendezések által rögzített adatok elemzése,
- sebezhetőség-vizsgálat (vulnerability analysis)
- behatolási tesztek (penetration testing) végzése
- feladatlap kitöltése,
- folyamatelemzés.

Az információbiztonság működésének ellenőrzése és mérése

Az ellenőrzések munkaszakaszai:

- előkészítés,
- felkészülés, helyszíni vizsgálat,
- írásba foglalás,
- hasznosítás, javaslatok (realizálás),

Az ellenőrzések jellegük szerint felosztatók:

- tervezett és rendszeres ellenőrzésekre,
- eseti vizsgálatokra,
- biztonsági esemény kivizsgálásokra.

Az információbiztonság működésének ellenőrzése és mérése

Vezetőségi vizsgálat,
szükséges információk:

- az auditok eredményeiről,
- a szakmai szervezetek, érintett felek visszajelzéseiről,
- a bevezetett megelőző és korrektív védelmi intézkedések aktuális állapotáról, azok bevezetésének hatásosságáról,
- a kockázatfelmérés során felvállalt, vagy maradványkockázatként feltárt kockázatokat, továbbá a kockázatkezelés során nem kezelt sebezhetőségi pontok és releváns fenyegetések listájáról,
- a mérési és ellenőrzési rendszer eredményeiről,
- a korábbi vezetőségi átvilágítás során tett intézkedésekről,
- bármilyen információbiztonságot ért változásról, és
- a fejlesztésre vonatkozó javaslatokról.

Az információbiztonság működésének ellenőrzése és mérése

Vezetőségi vizsgálat,
Tényeken alapuló döntéshozatal, irányul:

- a hatásosság fejlesztésére,
- a kockázatfelmérési, elemzési, kezelési tervek frissítésére,
- a működési eljárások módosítására, bevezetett kontrollokra,
- a szükséges erőforrások biztosítására,
- a mérési és ellenőrzési folyamatok fejlesztésére.

Az információbiztonság működésének ellenőrzése és mérése

Megfontolások a rendszerek biztonsági ellenőrzésére
Cél:

- maximalizálni a rendszert átvilágító auditálás hatékonyságát, és
- minimalizálni az általa vagy benne okozott zavarokat.
- intézkedéseket kell alkalmazni az üzemelő rendszer védelmére, és
- megóvjuk az auditálás alatt az auditáló eszközöket.
- védelmet kell alkalmazni ahhoz, hogy megóvjuk az auditáló eszközök sértetlenségét, és
- megelőzzük a velük való visszaélést.

Az információbiztonság működésének ellenőrzése és mérése

Ellenőrizni kell: az eszközök és értékük, az eszközökre irányuló fenyegetések és azok sérülékenységei és az eszközöket védő biztosítékok.

Az eszközöket az értékükben és az informatikai rendszerek biztonsági céljai változásának észlelése érdekében kell ellenőrizni. Ezeknek a változásoknak a lehetséges okai a következők: a szervezet céljai, az informatikai rendszerben működő alkalmazások, az informatikai rendszerben feldogozott információk és maguk az informatikai eszközök.

A fenyegetéseket és sérülékenységeket azért ellenőrizzük, hogy érzékeljük a változásokat súlyosságukban (például az infrastruktúrában, környezetben bekövetkezett változások okozhatják ezeket vagy technikai lehetőségek), és hogy korai szakaszban tudjunk érzékelni új fenyegetéseket vagy sérülékenységeket. Az eszközök változásai befolyásolhatják a fenyegetések és sérülékenységek változásait.

A biztosítékokat teljesítményük és hatékonyságuk vizsgálata érdekében ellenőrizzük időnként. Biztosítani kell, hogy megfelelőek legyenek, és az informatikai rendszert a szükséges védelmi szinten védjék. Lehetséges, hogy az eszközök, fenyegetések és sérülékenységek változásai befolyásolják a biztosítékok hatékonyságát és megfelelősségét.

Napló formájú kimenet az eseményekről.

Az információbiztonság működésének ellenőrzése és mérése

Rendszerauditálási óvintézkedések:

- Az átvilágító auditálás követelményeinek egyeztetése az illetékes vezetőséggel.
- Az ellenőrzés tárgyának rögzítése. (auditterv)
- A szoftverek és az adatok ellenőrzése a „csak olvasás” jellegű hozzáférésre legyen korlátozva.
- A „csak olvasás”-on kívüli hozzáférés kizárólag a rendszerállományok (rendszerfájlok) elkülönített, bizonyítható másolatán lehetséges, az átvilágító auditálás befejezésével. Ezeket az állományokat ajánlatos megsemmisíteni.
- Az ellenőrzéseket végző informatikai eszközöket pontosan kell azonosítani, és rendelkezésre kell bocsátani.
- A különleges vagy kiegészítő feldolgozás követelményeit ajánlatos azonosítani és egyeztetni.
- A hivatkozási napló (reference trail) készítéséhez ajánlatos minden egyes hozzáférést megfigyelni és naplózni (log).
- Valamennyi eljárást, követelményt és felelősséget ajánlatos írásba foglalni.

Az információbiztonság működésének ellenőrzése és mérése

Rendszerauditáló eszközök védelme:

- A hozzáférést a rendszerauditáló, átvilágító eszközökhöz, azaz szoftverekhez és adatállományokhoz (fájlokhoz) védeni kell annak érdekében, hogy kizárjuk a lehetséges visszaéléseket és a veszélyeztetést.
- Ezeket az eszközöket el kell különíteni az üzemeltető és a fejlesztő eszközöktől, és nem szabad azokat a szalagtárakban vagy a használói körzetekben tárolni, hacsak nincsenek ellátva alkalmas szintű kiegészítő védelemmel.

Köszönöm a figyelmet!

Informatikai Rendszerek Minőségbiztosítása és Auditja V.

Győrffyné Holló Krisztina
PE informatikai biztonsági szakértő, ISMS lead auditor
2021.10.08.

Témák

- 11. Az ISO/IEC 27001 Információbiztonsági Irányítási Rendszer szabvány követelményei és struktúrája;
- 12. Gyakorlatok, esettanulmányok.
- ZH

Informatikai Rendszerek Minőségbiztosítása és Auditja XI. Az Információbiztonsági Irányítási Rendszer szabvány

Győrffyné Holló Krisztina
PE informatikai biztonsági szakértő, ISMS lead auditor

Információbiztonsági irányítási rendszer követelmények

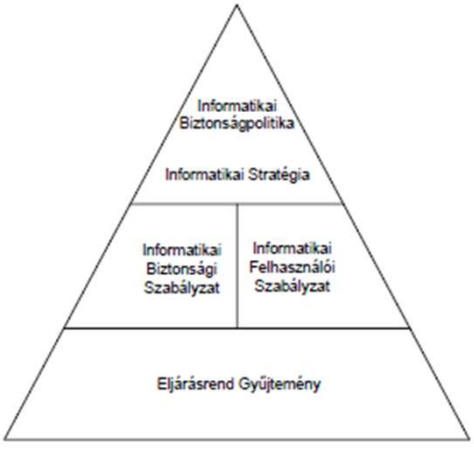
Felépítés:

(dokumentált irányítási rendszer)

- Vezetőségi elkötelezettség, Információbiztonsági nyilatkozat

(szándéknyilatkozat a bevezetésre és a működtetésre)

- Információbiztonsági politika
- Informatikai Stratégia (IFT)
- Szabályzat: ISZ, IBSZ, IFSZ
- Eljárások
- Szervezeti szereplők, felelősségek és hatáskörök



Információbiztonsági irányítási rendszer követelmények

Informatikai Biztonsági Szabályzat rögzíti

- az IBIR működéséhez, működtetéséhez szükséges folyamatokat,
- meghatározza az érintett szereplők
  - feladatait,
  - felelősségeit,
  - hatásköreit,
- rögzíti az információfeldolgozó rendszer elemeivel kapcsolatos biztonsági követelményeket.

Az egyes informatikai rendszerek esetében a szervezet Informatikai Biztonsági Szabályzata alapján az adott alkalmazási területen megvalósítandó, a fejlesztéssel és az üzemeltetéssel kapcsolatos tevékenységeket kell részleteiben szabályozni.

Információbiztonsági irányítási rendszer követelmények

Informatikai Biztonsági Szabályzathoz kapcsolódó dokumentumok:
Belső szabályozás:

- Szervezeti és Működési Szabályzat, szervezetek ügyrendje
- Iratkezelési Szabályzat,
- Biztonságtechnikai és Rendészeti Szabályzat,
- Tűzvédelmi Szabályzat,
- Munkavédelmi Szabályzat,
- Selejtezési Szabályzat (vagy előírás)
- Külső szabályozás:
- Jogszabályok

Információbiztonsági irányítási rendszer követelmények

Tartalmi követelmények:

- a szervezet vezetésének egyértelmű nyilatkozata az informatikai biztonság szabályozott kialakítására és fenntartására,
- az informatikai biztonság alapvető fogalmai,
- informatikai rendszerek és szolgáltatások biztonsági besorolása,
- elektronikus rendszerek meghatározása, biztonsági követelményeinek meghatározása (hozzáférés, alkalmazás, mentés…)
- elektronikus rendszerek fejlesztése,
- elektronikus kapcsolattartás szabályozása,
- adatvédelemi, adatkezelési, adattovábbítási előírások,
- az informatikai biztonsággal kapcsolatos feladat- és hatáskörök, felelősségek (jogok és kötelezettségek, szankcionálás),
- a biztonsági események jelentésének rendje,
- elektronikus naplózás szabályai,
- elvek, követelmények, kötelező eljárások, szabványok.

Információbiztonsági irányítási rendszer követelmények

Kapcsolódó előírások, szabályzatok:

- Felhasználói Szabályzat
- Rendszerüzemeltetői Szabályzat
- Telefon- és informatikai hálózat üzemeltetése
- Adatmentési előírások (elektronikus dokumentumok, informatikai rendszer adatbázisa)
- Eljárások: incidenskezelés, titkosítás, változáskezelés

- Iratkezelési Szabályzat
- Honlap szabályzat és Arculat kézikönyv
- Humánpolitikai Szabályzat (távmunka)
- Belső kontroll vagy audit szabályai

- Bizonylatok, űrlapok használata

- Elektronikus hibabejelentő rendszer
- Gépterem használati rend

Információbiztonsági irányítási rendszer követelmények

Informatikai Felhasználói Szabályzat

szabályozza

- a felhasználók jogait és kötelezettségeit az informatikai eszközök használata és a munkahelyi kapcsolattartás során,
- a felhasználó által elvégezhető és tiltott, elektronikus tevékenységeket,
- a szankcionálást (számonkérés feltétele, formája és módja),
- a naplózást és az incidenskezelést (biztonsági események bejelentési kötelezettsége),
- az informatikai szervezettel fenntartandó kapcsolati feltételeket (informatikai rendszerbeállítások, igénylések feltétele és folyamata).

- Felhasználói oktatások, tájékoztatók alapját képezi.

Információbiztonsági irányítási rendszer követelmények

Tartalmi követelmények:

- A szabályzat célja, érvényessége, hatályossága
- Felhasználók köre
- Felhasználói kategóriák
- Érintett informatikai rendszerek
- Hozzáférési jogosultságok: létesítés, módosítás, megszüntetés hozzáférési szintek meghatározása
- Elektronikus kapcsolattartás szabályai
- Adatvédelem (infotv., GDPR szabályai)
- Hibabejelentés szabályai
- Informatikai eszközök használata, igénylése – változáskezelés
- Elektronikus rendszerek használata
- Felhasználói jogok és kötelezettségek
- Fogalmak

Információbiztonsági irányítási rendszer követelmények

Az **eljárásrend gyűjtemény**be tartozó végrehajtási utasítások olyan alacsony szintű szabályzatok,

- amelyek részletesen és rendszer specifikusan rögzítik azokat a tevékenységeket, amelyeket az informatikai biztonsági szabályzat rendszertől függetlenül megkövetel,
- kidolgozása az adott szakterület vezetőjének kötelessége.
- Hatályba léptetése előtt érvényesítetni kell, véleményeztetés és jóváhagyás szükséges - az informatikai biztonsági tevékenységek koordinálásával megbízott vezető bevonásával.
- Az Informatikai Biztonsági Szabályzat rendelkezik a szükséges, az egyes szabályzati pontokhoz kötött eljárások kidolgozásáról és a felelős szervezeti egységről.
- Tájékoztatás, oktatás, munkaköri leíráshoz csatolás.
- Folyamatos fejlesztés és verziókövetés.

11

Információbiztonsági irányítási rendszer követelmények

Informatikai eljárások:

- Elektronikus dokumentumok mentése
- Adatmentés (rendszerek adatbázisa)
- Jogosultságkezelés és hozzáférés
- Honlapkezelés
- Levelezőrendszer és levelező lista rendszerének kezelése
- Iktatórendszer kezelése
- Gazdasági rendszer kezelése
- Rendszerüzemeltetése
- Telefon és Informatikai hálózati rendszer üzemeltetése
- Végponti adminisztrálói és szervízelés
- Rendszerek verziókezelése; Változáskezelés
- Konfigurációkezelés
- Licenckezelés
- Titkosítás

12

Információbiztonsági irányítási rendszer követelmények

Elektronikus dokumentumkezelés

Elektronikus dokumentumok:

- dokumentációk,
- jegyzőkönyvek,
- egyéb fájlok (kép, hang, video, folyamatábra, egyéb elektronikus információ – log, adatbázis, email…)

Követelmények

- a kezelésére, a védelmére, a felügyeletére vonatkoznak
- szakmai eljárások rögzítése és a követelmények alkalmazása
- kockázatelemző eljárások kidolgozása és alkalmazása, eredményeinek elemzése alapján kell meghozni az egyéb információvédelmi intézkedéseket is.

13

Információbiztonsági irányítási rendszer követelmények

Elektronikus dokumentumkezelés

Verziókezelés:

Bizonyíték szükséges, a meghatározott feladat kezelésére,

a legmegfelelőbb módszere a rögzítés:

- mikor és hol történik,
- milyenek a körülmények,
- ki mit csinált,
- és mi az eredménye.

Események rögzítése és a bizonyítékok megőrzése (papír vagy elektronikus formában).

Elektronikus verziókezelő rendszer.

Törvényi és szabványi megfelelés.

14

Információbiztonsági irányítási rendszer követelmények

A **vezetés hatásköre**:

- javaslattétel az informatikai vezető testület számára a stratégiai tervezéshez,
- az informatikai biztonsági irányelvek és feladatok vizsgálata és jóváhagyása, a megvalósításhoz szükséges humán és anyagi erőforrások biztosítása,
- az információs erőforrások súlyos veszélyhelyzeteknek való kitettségében bekövetkező jelentős változások nyomon követése,
- az informatikai biztonsági események nyomon követése,
- az informatikai biztonság fokozását szolgáló jelentős kezdeményezések jóváhagyása,
- az Informatikai Biztonsági Vezető személyének kijelölése, feladat- és hatáskörének meghatározása.

Információbiztonsági irányítási rendszer követelmények

Az **Informatikai Biztonsági Vezető** felelőssége az informatikai biztonság

- megtervezése,
- fenntartása,
- folyamatos fejlesztése.

Az erőforrások megszerzése és a védelmi intézkedések megvalósítása gyakran **más vezetők**re hárul a vonatkozó szabályozás alapján:

- (köz)beszerzési szabályzat
- Vagyonvédelmi/ biztonságtechnikai szabályzat
- Tűzvédelmi szabályzat stb.

Információbiztonsági irányítási rendszer követelmények

Biztonsági Vezető

- Gondoskodik az informatikai biztonságra vonatkozó jogszabályok, illetve az informatikai biztonságpolitika, az informatikai stratégia és az Informatikai Biztonsági Szabályzat végrehajtásáról, (szabályozási koncepciók, szabályzat tervezetek, szakmai állásfoglalás készítése)
- Szakmai szempontból véleményezi a szervezet szabályzatait és szerződéseit.
- Javaslatokat készít az informatikai biztonságpolitika, az informatikai stratégia és az Informatikai Biztonsági Szabályzat fejlesztésére.
- Gondoskodik az informatikai biztonságra vonatkozó rendelkezések betartásának rendszeres (legalább évente egyszeri) ellenőrzéséről, a lefolytatott ellenőrzések, vizsgálatok eredményéről tájékoztatja a szervezet vezetését.
- Irányítja és ellenőrzi az Informatikai Biztonsági Vezető munkáját.

17

Információbiztonsági irányítási rendszer követelmények

Informatikai Biztonsági Vezető

- Feladata a szervezet (szakterület, projekt, rendszer) által üzemeltetetett, illetve a szervezet (szakterület, projekt, rendszer) adatait feldolgozó informatikai és távközlési rendszerek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának
  - megteremtése,
  - fenntartása,
  - tervezése,
  - szervezése,
  - irányítása,
  - koordinálása és
  - ellenőrzése.

18

Információbiztonsági irányítási rendszer követelmények

Informatikai Biztonsági Vezető

- Felméri és elemzi a szervezet az informatikai biztonsággal összefüggő veszélyforrásokat, meghatározza a kockázatkezelés módszerét.
- Kidolgozza, és döntésre előterjeszti az informatikai biztonság kialakítására, a megfelelő informatikai biztonság elérésére, illetve fenntartására vonatkozó szabályokat, utasításokat, terveket és irányelveket.
- Rendkívüli események kezelésére szolgáló tervek elkészítése.
- Fizikai biztonsági feltételek kialakítása.
- Munkakörök betöltési szabályainak, feltételeinek meghatározása.
- Biztonsági követelmények és az előírások betartásának ellenőrzése - audit.
- Szakmai szempontból irányítja szervezetét, IT biztonsági oktatásokat bonyolít.
- Informatikai szabályzatokat véleményez, közreműködik.

19

Információbiztonsági irányítási rendszer követelmények

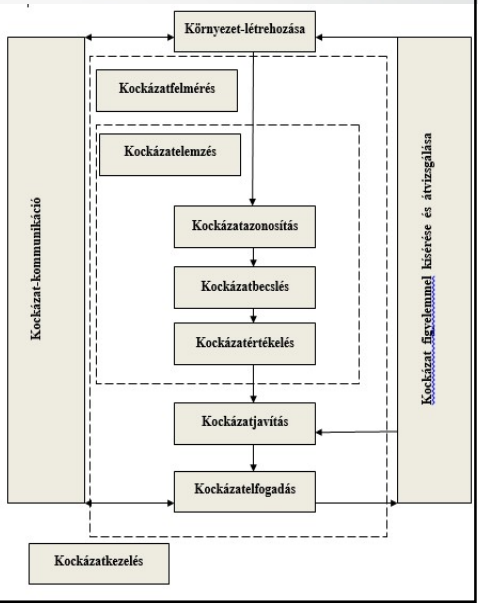
Mérőrendszer bevezetése

- Mérhető a bevezetett kontrollok hatékonysága és hatásossága
- Értékelhető a szervezet.

A mérési rendszert úgy kell kialakítani, hogy a kapott értékek összehasonlíthatók és a mérések megismételhetők legyenek.

Kockázatkezelési terv részei

- Kockázatfelmérési terv:
  - Kockázatelemzés
  - Kockázatbecslés
  - Kockázatértékelés
- Kockázatjavítási terv
- Kockázatelfogadás



Információbiztonsági irányítási rendszer követelmények

További feladatok:

- Stratégia megvalósítása: célok, erőforrás rendelkezésre állás
- Képzési és tudatossági oktatások:
  - oktatási és képzési dokumentáció, módszertani kézikönyv
  - résztvevők megfelelő kiválasztása
  - képzések hatásosságának mérése
- Feljegyzések kezelése
- Alkalmasság vizsgálata
  - Biztonsági követelmények érvényesítése a munkaköri leírásokban
  - Biztonsági átvilágítás
  - Titoktartás (célja, hogy felhívja a figyelmet az adott információk bizalmasságára)
  - Foglalkoztatás feltételei (általános és a munkakörre vonatkozó speciális biztonsági előírások)

Információbiztonsági irányítási rendszer követelmények

További feladatok:

- Gazdálkodás az erőforrásokkal

A vezetésnek a rendszer kialakításához, bevezetéséhez, működtetéséhez, felülvizsgálatához és fejlesztéséhez biztosítania szükséges a megfelelő erőforrásokat, mert hiányában a biztonság tekintetében megfogalmazott célok (biztonságpolitika) a gyakorlati érvényesítése kudarcra ítélt.

A rendszer bevezetése kapcsán a vezetésnek biztosítania kell mindazon erőforrásokat, melyek szükségesek a bevezetett kontrollok gyakorlatban történő érvényesítése és működtetése érdekében.

Információbiztonsági irányítási rendszer követelmények

Az Informatikai Biztonsági Irányítási Rendszer **irányítása**

- előírt feladatokat végre kell hajtaniuk,
- az irányítást végző vezetésnek visszacsatolással kell rendelkeznie a bevezetett kontrollok működőképességéről, azok hatékonyságáról
- ellenőrző, mérő rendszer kialakítása
- tényeken alapuló döntéshozatal: A vezetés a kapott információk alapján dönt a szükséges módosítási fejlesztési irányok meghatározásáról.
- folyamatos változás, fejlődés
- ki kell kijelölni fejlődési folyamatot, amelyhez alapvetően szükséges az irányítási tevékenységek ellátása.

23

Köszönöm a figyelmet!