HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI
SZAKOSZTÁLY

Az Információbiztonsági vezető sajátos helyzete, szerepe, az érdekelt felekkel való kapcsolata és együttműködése a gyakorlatban

Nagy Sándor
TrustaaS Kft., szenior IT biztonsági tanácsadó

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Ki az IT biztonsági felelős és mi a feladata?

- Ibtv.: 11§: „A szervezet vezetője … az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg …
- 13§ (2) Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:
  - gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
  - elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
  - előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
  - előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
  - véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
  - kapcsolatot tart a hatósággal és az eseménykezelő központtal.
  - …a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Ki az IT biztonsági felelős és mi a feladata?

- (5) Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az e törvényben meghatározott követelmények teljesülését
  - a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,
  - b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők

  e törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.
- A (2) bekezdés és alpontjai inkább az adminisztratív feladatokat taglalják,
- Az (5) bekezdésben foglaltak elvégzése viszont operatív munkavégzést igényel – az IT üzemeltetés felügyeletét, tanácsadást és konzultációt az IT-val, szerepvállalást az IT fejlesztésekben.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Mi lehet az IBF munkaköre egy adott szervezetnél?

Az Ibtv. szerint:

- „A szervezet vezetője meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat!”

Bár az Ibtv. egyértelműen fogalmaz, az IBF helyét és szerepét különböző vezetői és szervezeti motivációk is befolyásolják.

Vezetői motivációk:

- Törvényi kötelezettségeknek való megfelelés,
- Auditon való megfelelés,
- Az IT tevékenységének segítése,
- Az IT tevékenységének átlátása (belelátás az IT működésbe),
- Az IT tevékenységének kontrollja.

A munkaköri leírás tükrözi az elsődleges vezetői szándékot!

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Mekkora valójában az IBF hatásköre?

- Az Ibtv. normaszövege látszólag egyértelműen fogalmaz – de lehetnek helyi adaptációs különbségek.
- A BM rendelet jelentősen pontosít a feladatokon – elég csak a 4-es mellékletben szereplő védelmi intézkedési katalógusban előírt feladatokat átnézni:
  - IBSZ kialakítása, betartása és betartatása,
  - Kockázatelemzés(ek) készítése,
  - egy tucat olyan eljárásrend kialakítása, betartása és betartatása,
  - A fejlesztések felügyelete, amikben érvényre kell juttatni a szabályozók szellemiségét.
- A GDPR IT biztonság ügyben nagyon szűkszavúan fogalmaz, de nagyon súlyos feladatokat szab
  - a szervezet köteles megtenni minden tőle telhetőt a személyes adatok védelmére,
  - a természetes személyek számára biztosítani kell a GDPR-ban előírt jogok teljesülését.

Tehát nemcsak a teljes IT működés tartozik az IBF felügyelete alá, de a GDPR érintettség révén minden olyan folyamat is, ami informatikával támogatott módon személyes adatokat kezel.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Mik az IBF tevékenység által érintett/érintendő területek?

- A napi szintű informatikai üzemeltetés, az IT működése, az üzemeltetett eszközök és rendszerek
- A cégen belül, vagy a cég érdekében végzett eszköz- és alkalmazásfejlesztési tevékenységek
- Az informatikai eszközök és rendszerek alkalmazása és felhasználása a cégen belül
- Az informatikai eszközökkel és rendszerekkel támogatott üzleti folyamatok
- Az üzleti folyamatok elvégzéséhez szükséges információk, a folyamatokban végrehajtott adatkezelések, a kezelt adatvagyon, az adatvagyon informatikai megjelenési módjai
- Az informatikai működés és az üzleti igények kapcsolódásai – igénylések, igénykezelési folyamatok
- Az üzleti folyamatok fenntarthatósága, sérülékenysége, a működésfolytonosság biztosítása

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Kik az IBF tevékenységében az „érdekelt felek”?

- Informatikai üzemeltetők – külsős és belső munkatársak
- Informatikai fejlesztők - külsős és belső munkatársak
- Alkalmazásgazdák, kulcsfelhasználók
- Informatikai vezetés
- Informatikát érintő projektek tagjai, vezetői
- Jogi és biztonsági terület munkatársai
- Belső ellenőrzés
- Auditorok
- Hatóság

- és természetesen a Közvetlen felettes

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Az IBF lehetséges előzetes megítélései

- A felesleges rossz (ahol az IT mindent tud, és mindent tökéletesen csinál)
- A szükséges rossz –(ahol az IT mindent tud, de meg kell felelni a törvényes előírásoknak)
- Az ember, aki majd kontrollálja az IT működést (különösen outsource esetében)
- Az ember, aki majd megfékezi az IT-t, aki rendet tesz (ha nagy az IT dominanciája)
- Aki majd behurcolja – vagy fokozni fogja – a paranoiát
- Aki kerékkötő lesz a megszokott működésben

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Hogyan fogadtassuk el magunkat IBF-ként a cégen belül?

- Próbáljuk megismerni a cég tevékenységét minél mélyebben – ha másképp nem megy, az IT szemszögén keresztül.
- Csináljunk interjúkat az IT-n belül, hogy megismertessük magunkat a kollégákkal, és mi is megismerjük őket és a munkájukat.
- Az összeálló kép alapján tekintsük át a meglévő szabályozást, tegyünk javaslatot annak módosítására.
- Végezzük el a szabályzat-módosításokat, adjuk ki őket bírálatra.
- Jelentkezzünk be a problémás esetekért, a vitás kérdésekért – a normaszöveg értelmezése iránymutatást ad(hat) a napi üzemeltetésnek is.
  - Ehhez négy szabályozót kell tartalmilag és „szellemiségében” jól ismerni: Ibtv., BM rendelet, GDPR, ISO 270xx. (Na és persze a NIST)
- Próbáljunk kapcsolatot találni a társ-területekkel – ebben jó kapaszkodó lehet a GDPR.
- Főnökünk szemében jó pont, ha igyekszünk magunkénak érezni feladatokat, megnyilvánulunk minket érintő kérdésekben (akkor is, ha csak közvetve vagyunk megszólítva), átvállaljuk vezetőnk munkájának az ITB vonatkozású részeit.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Hogyan lehet egy IBF hiteles a partnerek szemében?

- Ismerjük alaposan az Ibtv. és a BM rendelet normaszövegeket – és persze az ISO 270xx és a GDPR előírásait is.
- Ismerjük, tudjuk a cég és a céges IT tevékenységét.
- Érjük el, hogy IT biztonsági szempontból problémásnak látszó kérdésekkel megkeressenek minket
  - Ehhez felelősséget kell vállalni,
  - A kibukott IT biztonsági problémák megoldását magunkévá kell tenni, és amiben lehet, lépni kell – ha másképp nem, legalább akcióterv szinten.
- Próbáljunk hozzáférést kapni – betekintési joggal – felügyeleti rendszerekhez
  - Így láthatjuk, mi történik, segíthetünk kényes helyzetekben, napi kapcsolatot tarthatunk az üzemeltetéssel.
- Kérdezzünk, tájékozódjunk, nézzünk utána. **Mottó:** nem érthet mindenki mindenhez, azért van a Wikipédia.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

„Meddig fokozzuk a paranoiát"?

- A vezetőség, az üzemeltetés, az alkalmazás fejlesztés a saját rutinja szerint szeret működni, működtetni, fejleszteni.
- Ma már nemcsak a vállalkozói szféra akar trendi lenni.
- Az állami vezetőkön éppúgy rajta van a haladás kényszere, mint a vállalati vezetőkön.
- A költségérzékenység sajnos nem éppen az IBF barátja.

Nagyon fontos, hogy mindezeket figyelembe vegyük az IBF tevékenységünk során

Mottó: Nincs baj, amíg nincs BAJ.

Kérdés: Ki a felelős, ha elér minket a végzet?

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

„Meddig fokozzuk a paranoiát"?

Konklúzió:

- Próbáljunk a lehetőségeken belül maradva hatékony rendszert építeni – inkább csak kisebb beszerzéseket megvalósítani, és csak a legszükségesebbeket.
- Ismerjük az üzemeltetett rendszereket, és próbáljunk azokra akár napi szinten odafigyelni, így fokozva az üzemeltetés éberségét.
- Találjunk kapcsolatot be az beszerzésekhez, a fejlesztésekhez, és ismertessük meg a törvényi követelményeket az ebben résztvevő partnerekkel is.
- Ne csak az üzemeltetésre figyeljünk, hanem a munkafolyamatokra is – ezt a GDPR és az ISO is megköveteli tőlünk.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Hogyan építsünk és tartsunk fenn IBIR-t?

- Mérjük fel a hiányosságokat és a lehetőségeket.
- Tekintsük át a szabályzatokat. Ami hiányzik, de egyszerűen lehet és élhető módon lehet szabályozni, azt szabályozzuk le. Ami van, de nehézkes, tegyük élhetőbbé – de ne áldozzuk fel a biztonságot a népszerűségért.
- Szabályzatainkat oktassuk – vagy legalább ismertessük – de legyenek kontroll pontjaink, ahol a betartásukat ellenőrizzük. A folyamatos jelenlét többet ér.
- Ha vannak workflow-k, a ránk is tartozó feladatokat tereljük magunk felé.
- Kérjünk betekintési jogosultságot a felügyeleti rendszerekhez.
- Kérdezzünk rá a monitorozás során tapasztalt anomáliákra.
- Vegyük komolyan a magunk által leírtakat – kérjük számon a feladatok elvégzését (legyen az patch management, vagy jogosultság kezelés).
- Váljunk a kollektíva részévé – ahol ITB is érintett egy döntésben, ott vállaljuk fel a döntést, és indokoljuk is meg. Ha ránk kérdeznek – döntsünk.
- Legyünk következetesek. Ha valamiért el kell térni a kívánatostól, azt a külvilágnak indokoljuk meg és dokumentáljuk.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Kik segíthetnek minket, hogyan és miben?

- Legyenek szövetségeseink az IT munkatársai. Fontos, hogy bízzanak bennünk. Tőlük lesznek szabályozóink életképesek.
- Legyen állandó kapcsolatunk a beszállítókkal – segítik naprakészségünket, és jó háttér tudásbázist adhatnak.
- Nagyon fontos, hogy minden projekt úgy fusson le, hogy a megfelelő ITB dokumentumok el lettek készítve.
  - Az ITB dokumentumok elvárt tartalma az Ibtv-ből (BM rendelet, 4 melléklet) nagyon pontosan kiolvasható,
  - Ha valamilyen dokumentum tartalmában, felépítésében nem vagyunk biztosak, kérjük ki a beszállító tanácsát – hátha volt már ilyen az ő praxisában,
  - Ha nincs ilyen tudása, időben jelezzük, hogy erre is szüksége lesz (pályázati kiírás!),
  - Ha ITB tanácsadó cég segítheti a munkánkat, akkor ne a leendő partner neve vezessen minket, hanem a referenciái, a projekttapasztalata. Érdemes személyes konzultáción meggyőződni a valós tudásról és háttérről. Kérjünk be minta dokumentumokat a tanácsadótól (valódi tartalmút, csak anonimizáltat), mert az mutatja a valódi tudást.
- Főnökünk, vezetőnk tudja és higgye, hogy amit csinálunk az a napi léthez fontos!

HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI
SZAKOSZTÁLY

Köszönöm a figyelmet!