

Mennyire hihetünk az információbiztonsági felméréseknek?

Adatok gyűjtése és feldolgozása: 2015-2021

Dombora Sándor

2022.09.14.

Az ISACA Magyarországi Egyesület által szervezett Második szerdai előadásokon bármilyen eszközzel történő kép- vagy hangrögzítés tilos. (Idetartozik a mobiltelefonokkal készített kép- vagy hangfelvétel is). A jelen szabály be nem tartása szerzői- és szomszédos jogi jogsértés jogkövetkezményeit vonhatja maga után.

Confidential. For internal use only.

FELELŐSSÉG KIZÁRÁSA

Az elhangzott prezentációk tartalmát illetően az ISACA Magyarországi Egyesület nem vállal felelősséget az abban nyújtott információk aktualitásáért, helyességéért és teljességéért.

Az itt elhangzott információk nem feltétlenül egyeznek meg az ISACA Magyarországi Egyesület álláspontjával.

Felmérések és statisztikák

- Általános felmérés
- Szakterületre vonatkozó felmérés
- Tanácsadói statisztikák
- Gyártói statisztikák
- Hatósági statisztikák

Általános felmérések

- Átfogó (minden részterületre kiterjed)
- Magas szintű (megmarad a részterületek szintjén)
- Részlethiányos (nem részletezi az egyes részterületeket)
- Célja: általános információbiztonsági helyzetkép
- Publikálók: tanácsadó cégek, ISACA

Szakterületre vonatkozó felmérés

- Jellemzően az adott szakterületet dolgozza fel
 - Biztonságtudatosság
 - Információbiztonsági szabályzat/eljárás
 - Biztonsági szervezet
 - Gazdasági szektor felmérése
 - Stb.
- Részletes feltárása az adott szakterületnek
- Célja szakterület fejlődésének bemutatása, marketing
- Publikálók: tanácsadó cégek, gyártók

Tanácsadói statisztikák

- Általános és szakterületi
- Részletes, magas szintű vagy fókuszterületre vonatkozó
- Célja:
 - Általános információbiztonsági helyzetkép
 - Szakterület fókuszba helyezése
 - Marketing (a tanácsadó fókuszterületére vonatkozóan, gyártó népszerűsítése)
 - Stb.
- Publikálók: tanácsadó cégek

Hatósági statisztikák

- Általános és szakterületi
- Részletes, magas szintű vagy fókuszterületre vonatkozó
- Célja az ágazat információbiztonságának:
 - Felmérése
 - Publikálása
 - Fejlesztése
 - Hatósági előírások fejlesztése
- Készítők/Publikálók: hatóságok

Gyártói statisztikák

- Adott információbiztonsági megoldás szegmensére vonatkozik
- Belemegy a részletekbe (termék/megoldás erősségeit illetően)
- Az adott gyártó termékének tulajdonságaira fókuszál
- Mellőzi a gyártó termékeinek gyengeségeire vonatkozó témákat
- Célja az adott gyártó termékeinek népszerűsítése
- Publikálók: gyártók

Adatok forrása

- Kérdőívek kitöltése
 - Telefonos felmérés
 - Kiküldött és begyűjtött kérdőívek: célszervezet általi önálló kitöltés
 - Kérdezőbiztos általi kitöltés a célszervezettel közösen
- Tanácsadói projektek
 - Tapasztalaton alapul
 - Szakértők a szervezetről elérhető ismerete alapján
- Termékek eladása és használatának visszacsatolása
 - Tapasztalaton alapul
 - Visszajelzések pontossága

Adatok torzulása - Telefonos felmérés és Kiküldött kérdőív

- A felmérés módja miatt
 - Elért személy nem tud hiteles adatokat szolgáltatni
 - Szolgáltatott adatok megbízhatósága nem ellenőrizhető (szépítés, ismerthiány)
 - A mintavétellel kiválasztott szervezetek reprezentativitása (módszertani hiányosságok)
 - Szervezet méretek keveredése (1-2 fős szervezetek)
- A szervezet érdekei - titokban tartani a hiányosságokat
 - Megelőzni a hiányosságok kihasználását
 - Jobb képet mutatni a szervezetről (image)
 - Eltitkolni a hiányosságokat a hatóságok elől (büntetések elkerülése)

Adatok torzulása – Helyszíni kérdezőbiztos

- A felmérés módja miatt
 - Elért személy nem tud hiteles adatokat szolgáltatni
 - Szolgáltatott adatok megbízhatósága nem ellenőrizhető (szépítés, ismerthiány)
 - A mintavétellel kiválasztott szervezetek reprezentativitása (módszertani hiányosságok)
- A szervezet érdekei - titokban tartani a hiányosságokat
 - Megelőzni a hiányosságok kihasználását
 - Jobb képet mutatni a szervezetről (image)
 - Eltitkolni a hiányosságokat a hatóságok előtt (büntetések elkerülése)

Adatok torzulása – Tanácsadói projektek

- A felmérés módja miatt
 - A projektben részt vevő személyektől származó információ nem hiteles
 - Az információ tanácsadó általi félreértelmezése
 - A mintavétel a projektekben részt vevő cégekre korlátozódik
 - A mintavétel nem reprezentatív
- A szervezet érdekei - titokban tartani a hiányosságokat
 - Megelőzni a hiányosságok kihasználását
 - Jobb képet mutatni a szervezetről (szépítés)
 - Eltitkolni a hiányosságokat a hatóságok előtt (szépítés a büntetések elkerülése érdekében)

Adatok torzulása – Gyártói felmérések

- A felmérés módja miatt
 - A szervezettől származó információ nem hiteles
 - Az információ gyártó képviselője általi félreértelmezése
 - A mintavétel a gyártó látókörébe tartozó cégekre korlátozódik
 - A mintavétel nem reprezentatív
 - Marketing célok miatt a kérdőív torzítja a szakterület
- A gyártó érdekei – minél jobb marketing/minél több eladás
 - Megelőzni a hiányosságok kihasználását
 - Kiemelni a termék használatának előnyeit (szépítés)
 - Elhanyagolni a termék hiányosságait, használatának buktatóit (szépítés)
 - Statisztika torzítása a termék jobb értékelése érdekében (jellemzően félreérthető)

Az adatok további torzulása

- Kvantitatív adatok (a legtöbb kérdés a felmérésben)
 - Van vagy nincs a kontroll?
 - Felelős: Rendelkezik végzettséggel? Rendelkezik tapasztalattal?
- Kvalitatív adatok– meglévő biztonsági intézkedések végrehajtása
 - A kontroll struktúra jól definiált?
 - A kontroll be van építve a szervezet működésébe/illeszkedik a szervezet felépítéséhez?
 - A kialakított szabályzat/eljárásrend/kontroll érthető és értelmezhető?
 - A kontroll működőképes?
 - A kontroll végrehajtható és eléri a célját vagy csak papíron létezik?
 - Ütközik az üzleti érdekekkel?

Az adatok torzulásának megfigyelése

- Kvantitatív adatok (a legtöbb kérdés a felmérésben)
 - Van vagy nincs a kontroll?
 - Felelős: Rendelkezik végzettséggel? Rendelkezik tapasztalattal?
- Kvalitatív adatok– (kevesebb kérdés/pontatlan és torzított válaszok)
 - A kontroll struktúra jól definiált?
 - A kontroll be van építve a szervezet működésébe/illeszkedik a szervezet felépítéséhez?
 - A kialakított szabályzat/eljárásrend/kontroll érthető és értelmezhető?
 - A kontroll működőképes?
 - A kontroll végrehajtható és eléri a célját vagy csak papíron létezik?
 - Ütközik az üzleti érdekekkel?

Az adatok további torzulása – Információbiztonsági problémák

Meglévő szabályzatrendszer problémái	Előfordulás (7 minta)
Strukturális problémák	7
szabályzat hierarchia hiányosságai	6
szerepkörönkénti szegmentálás hiánya (kire vonatkozik, ki hajtja végre)	5
túlméretezett szabályzatok	1
nem releváns tartalom	1
Értelmezhetőségi problémák	7
fogalomtár és rövidítésjegyzék hiánya	4
ismeretlen szakszövegek	5
Megfelelőségi problémák	7
nem illeszkedik a jogi és üzleti elvárásokhoz	6
megfelelés ellenőrzési nehézségek	6
Alkalmazhatósági problémák	7
belső ellentmondások	2
ellentmondások az üzleti folyamatoknak (nincs összehangolva, blokkolja a folyamatok végrehajtását)	7
valóságtól elrugaszkodott (nem állnak rendelkezésre a szükséges erőforrások)	4
túl általános (jogszabály/szabvány másolata)	5
irreleváns a környezetre (valahonnan másolták)	2
Redundancia problémák (legkevésbé fontos)	7
redundáns kockázatkezelés – különböző módszertanok és skálák szerint	7
redundáns incidenskezelés – koordináció és kommunikáció hiánya	7

Felmérések jellemzőinek összesítése

Felmérés típusa	Mintavételi lehetőség	Kapcsolat a célszervezettel	IB problémák figyelembe vétele	Reprezentatív felmérés	Felmérés megbízhatósága
Telefonos felmérés	független	Nincs	Nem	Igen (Mintavételtől függően)	alacsony
Kiküldött kérdőív	független	Nincs	Nem	Igen (Mintavételtől függően)	alacsony
Helyszíni kérdezőbiztos	kis és közepes minták	Eseti	Részben	Igen	közepes
Tanácsadói projektek	kis és közepes minták	Eseti/Közvetlen	Igen	Nem	magas
Gyártói statisztikák	termék elterjedtsége	Eseti/Közvetlen	Nem	Nem	közepes

Miért jó mégis, hogy van?

- Általános információbiztonsági helyzetkép
 - Bemutatja a kontrollok létezését (van/nincs)
 - Nem veszi figyelembe az IB szabályzatrendszer problémáit vagy nem reprezentatív
 - Összegzi az elérhető információt az információbiztonság állapotáról
 - A felmérések általában jobb képet mutatnak a valóságnál
- Kontextusba helyezve kell értelmezni a felmérések eredményét
 - A hol tartunk a versenytársakhoz képest megválaszolása ösztönzi az információbiztonság fejlesztését
 - A felmérésekre való támaszkodás a szabályzatrendszer problémáinak figyelmen kívül hagyása esetén hamis biztonságtudatot eredményez



KÖSZÖNÖM A FIGYELMET!