Információbiztonság tudatosság fejlesztése a gyakorlatban

Bubán Márton

2019. október 24.

INFORMÁCIÓBIZTONSÁG SZEREPE

Az információ birtoklásával járó előnyt Szun-Vu fogalmazta meg „Szun-Ce: A háború művészete” című művében a legtalálóbban:

„Ezért mondják, hogy aki ismeri az ellenséget és ismeri önmagát, száz csatában sem kerül veszélybe. Aki nem ismeri az ellenséget, ám ismeri önmagát, egyszer győz, másszor kudarcot vall. Aki sem az ellenséget, sem önmagát nem ismeri, minden csatában vereséget szenved.”

(Szun-Vu, 2006 (i. e. 514–496))

KÉPZÉS RENDSZERÉNEK KIALAKÍTÁSA

1. szervezeti, célcsoportot érintő lehatárolás
2. a tartalmi elemek kialakítása
3. az oktatás formájának, módszertanának meghatározása
4. számonkérés, a visszamérés követelményeinek rögzítése
5. dokumentálás kereteinek kialakítása

SZERVEZETI, CÉLCSOPORT SZERINTI LEHATÁROLÁS

Valamennyi információs rendszert használó munkatárs

- egységes alapképzés

Valamennyi erőforrás, illetve folyamatgazda

- vezetői elkötelezettség és támogató szerep erősítése
- a minőségszemélet,
- az informatikai biztonság, biztonságszemlélet
- a kapcsolódó szabályozók ismerete,
- az incidens, katasztrófa, ügymenet folytonosságot érintő szerep

Valamennyi, információbiztonság szempontjából operatív feladatellátással érintett munkatárs

- elvárt információbiztonsági magatartások erősítése,
- incidenskezelés operatív végrehajtásával kapcsolatos tevékenységek fejlesztése,
- kapcsolódó szabályozási környezet ismerete és a benne foglaltak alkalmazása,
- információbiztonsági kontrolloknak történő megfelelőség

OKTATÁS FORMÁJÁNAK MEGHATÁROZÁSA

Általános információ biztonság tudatosság fejlesztő képzés

[*e-learning, alapképzés, valamennyi felhasználó részére: belépéskor, illetve évente legalább egy alkalommal*]

Információbiztonság megteremtésében, fenntartásában érintett résztvevők részére kiegészítő kurzus

[*e-learning, kompetenciafejlesztés, közreműködők részére*]

Vezetői kiegészítő kurzus

[*e-learning, kompetenciafejlesztés, vezetők részére*]

Informatikai üzemeltető kör részére workshop

[*jelenléti, informatikusok részére, évi 2 alkalommal*]

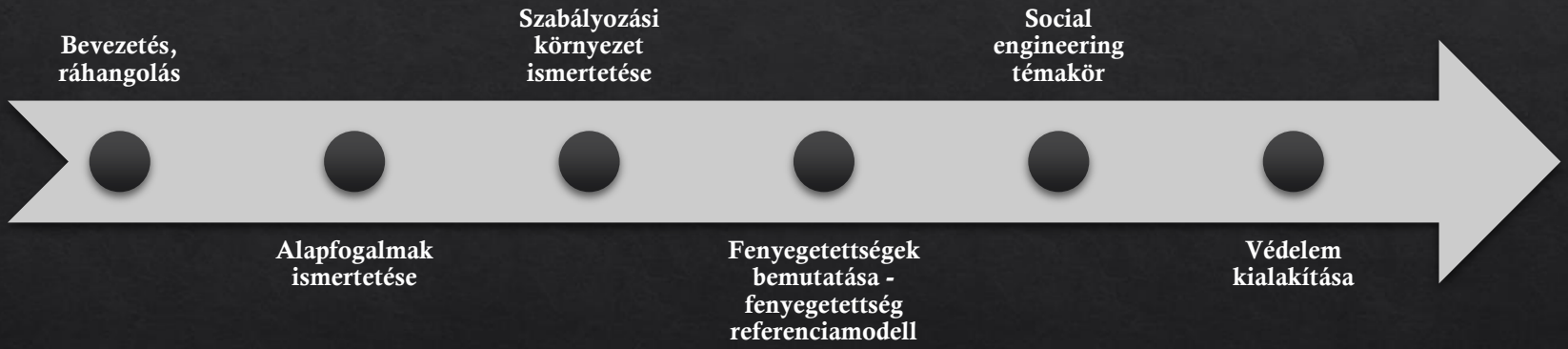
Biztonsági személyzet részére workshop

[*jelenléti, biztonsági személyzet részére, évi 2 alkalommal*]

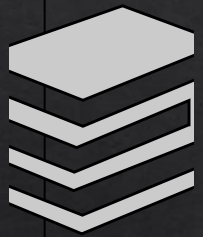
Vezetők részére konzultáció

[*jelenléti, vezetők részére, évi 3 alkalommal*]

TARTALMI ELEMEK - ALAPKÉPZÉS



TARTALMI ELEMEK - OPERATÍV FELADATELLÁTÓK KÉPZÉSE



Szabályozási környezet: a feladatellátásban részt vevők vonatkozásában megkövetelt elemei:

- felhasználói jelzések kezelése,
- kommunikációs formák és csatornák,
- incidenskezelés eljárásrend protokoll szintű elemei,
- felhasználók jogai, feladatai, kötelezettségei,
- üzemeltetők, biztonsági személyzet, incidenskezelők jogai, feladatai, kötelezettségei;

Fenyegetettségek kezelése: az információbiztonságot érintő eljárásrendek ismertetése:

- fizikai biztonság,
- informatikai üzemeltetés,
- incidenskezelés területén;

Kommunikáció, stresszkezelés:

- információbiztonságot érintő operatív feladatellátás során elvárt viselkedés,
- asszertív kommunikáció,
- stresszel járó szituációk kezelése.

Social engineering: (gyakorlati példákon, esettanulmányokon keresztüli megközelítés):

- az üzemeltetési területen kockázatként megjelenő humán ,
- számítógép alapú technikák.

TARTALMI ELEMEK - OPERATÍV FELADATELLÁTÓK WORKSHOP

Informatikai üzemeltetés, incidenskezelés **területén** dolgozó munkatársak részére **incidenskezeléssel kapcsolatos** (detektálás, első lépések, elhárítás, tapasztalatok levonása, megszerzett tudás integrálása) **ismeretek gyakorlatban történő elsajátítása**, szimulált környezetben, „játékos" elemek segítségével.

Biztonsági személyzet részére a fizikai biztonság környezetével kapcsolatos ismeretek elmélyítésére, a területre jellemző kockázatok, fenyegetettségek kezelésére vonatkozó tartalmi elemekkel, gyakorlati példákon keresztüli megközelítésben (shoulder surfing és dumpster diving, tailgating, piggybacking módszerek, objektumvédelem, védendő adatvagyon elemei, adatvédelmi kérdések, szabadulószoba).

Szabályozókkal, szabályozási környezettel kapcsolatos **feladatkataszter, RACI felelősségi tábla gyakorlati bemutatása**

TARTALMI ELEMEK - VEZETŐI E-LEARNING

Szabályozási környezet: a szervezet és adatvagyon védelmének szemszögéből

- jogszabályok, szabványok, ajánlások, információ-biztonsági, adatvédelmi, szabályozó dokumentumok
- Felhasználói és vezetői szinten meghatározott kötelesség – felelősség rendszerét
- Követelményeit, a normasértés következményeit.

Social engineering: a támadással összefüggő pszichológiai manipulációs eszköztár kibontása, illetve a védekezési technikák ismertetése során az alábbi témakörök részletes kifejtése

- Adathalász technikák pszichológiai hátterének, kommunikációs eszköztárának a bemutatása;
- Nézőpont váltás, mely a támadó oldaláról világít rá a biztonság alapvető kérdéseire;
- érintett részéről árulkodó jelek elrejtésére, a testbeszéd utalása;
- a támadó testbeszédében a manipulációs szándék felismerése.

TARTALMI ELEMEK - VEZETŐI KONZULTÁCIÓ

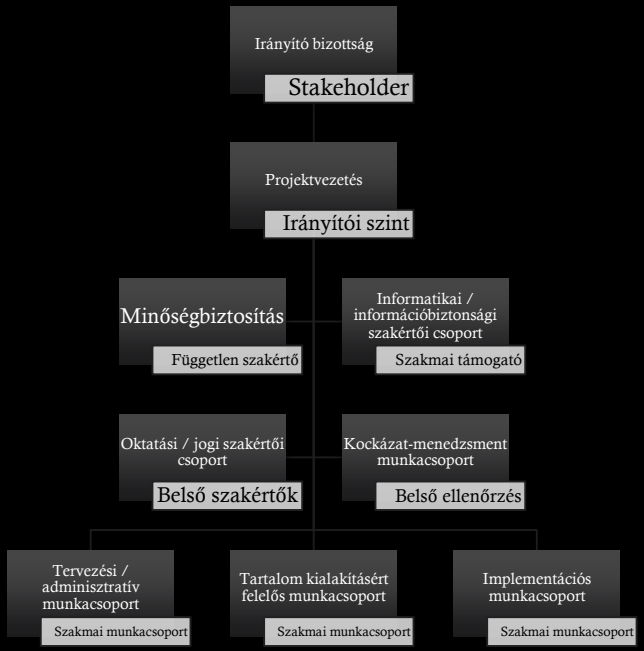
Az **információbiztonságot érintő szabályozók szervezeti szintű hatásai** kapcsán felvetődött kérdések témájában javaslom a konzultációs forma alkalmazását.

A kurzus másik felében, **pszichológus, illetve social engineer szakértő bevonása mellett** a vezetői e-learning képzésben megjelölt **social engineering** témákban tervezem a szerepjátékelemekkel gazdagított **szituációs gyakorlatok** levezetését.

Kurzus megnevezése	Forma	Résztvevők köre	Előzetes szintfelmérés	Kurzus zárásának feltétele
Alapképzés	E-learning	Valamennyi felhasználó	Igen	Sikeres záróvizsga
Alapképzést kiegészítő jelenléti konzultáció	Jelenléti	Valamennyi felhasználó	Nem	Aktív résztvétel
Információbiztonság operatív szereplői számára tartott képzés	E-learning	Informatikus, biztonsági személyzet	Nem	Sikeres záróvizsga
Információbiztonság operatív szereplői számára tartott workshop	Jelenléti	Informatikus, biztonsági személyzet	Nem	Aktív résztvétel
Vezetői e-learning kurzus	E-learning	Vezetők	Nem	Sikeres záróvizsga
Vezetői konzultáció	Jelenléti	Vezetők	Nem	Aktív résztvétel

VISSZAMÉRÉS RENDSZERE

MEGVALÓSÍTÁS – PROJEKTSZERVEZET



TOVÁBBI ESZKÖZÖK

- Rendszeres hírlevél
- Soron kívüli tájékoztató levél
- Normatív utasítások, tájékoztatók kiadása
- Információ-biztonsági tematikájú aloldal
- Kampányok, versenyek, vetélkedők
- Információ-biztonsági szakmai nap
- Tréningek feladatellátók részére
- Rendszeres értekezlet / workshop
- Szervezeti rendezvényekre „beinjektálás”
- Adathalász szimuláció
- Felhasználói visszamérések
- PDCA: ticketing rendszeren
- Incidenskezelési gyakorlatok
- Log alapján visszacsatolások a felhasználók felé
- Véleményvezérek megnyerése

MÁSODLAGOS HATÁSOK I

- A képzés eredményeként kialakult új ismeretek következtében a szervezeten belüli tematikus kommunikáció által, a **közösségi tudás fejlődése útján a szervezeti kultúra szintjére gyűrűzik be az elsajátított tudás**.
- A valamennyi felhasználó részére kötelező módon kiterjesztett képzés közösen megélt ingerek, érzelmek mellett **közös célok jelennek meg**: a szervezeten belül a formális kapcsolati szint mellett az informális szinten is **új kapcsolatok kialakulását segíti, így vélemény és szervezetformáló hatása lesz.**
- Egy statikus, szakmai feladatellátással foglalkozó szervezetben **gondolatébresztő, vitatára ösztönző képzés, inspiráló, fejlődésre ösztönző légkör kialakulásához vezethet**.

MÁSODLAGOS HATÁSOK II

- Az egyes feladatellátás és szerepkör által lehatárolt csoportokra kialakított kurzusok alkalmával, a workshop és konzultáció oktatási formák által teremtett **szabad, alkotói légkör hozzájárul a munkatársak szervezeti elköteleződéséhez, eszköz lehet a fluktuáció mérsékléséhez.**
- A képzési rendszer egésze alkalmas arra, hogy **a szervezet munkatársai** a közösen végzett, illetve egymásra épülő feladatellátás során, az **adott információbiztonságot érintő területet eltérő nézőpontokból látva, a mások nézőpontjának megismerése révén lokális szinten szinergikus, egymást erősítő hatás kialakulását segítse elő**.

ZÁRÓ GONDOLATOK

A képzési egészére, struktúrára, tananyagra nem szabad úgy tekinteni, mint egy kész termékre, hanem – integráltan a szervezet információbiztonsági irányítási rendszerével – folyamatosan javítani, fejleszteni szükséges. PDCA elv alkalmazásával a környezeti és belső igényekhez igazítandó, a szervezet információbiztonsági érettségét alapjaiban meghatározó erőforrásként kell kezelni.

Preventív elemként alkalmazva, az incidens megelőzésének egyik fontos eszközeként, a szervezeten belül kiemelt folyamatként kell rá tekinteni:

„A bölcs hadvezér rákényszeríti akaratát az ellenségre, de nem engedi, hogy az ellenség ugyanezt tegyeővele.”

(Szun-Vu, 2006 (i. e. 514–496))

Köszönöm a figyelmet!