HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztése

Nagy vonalakban egy szervezet információbiztonsági kultúrájának fejlesztéséről

Bubán Márton

EIVOK-6. Információbiztonsági Szakmai Fórum

2018.10.04

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság szerepe

Az információ birtoklásából, az önmagunk képességeinek ismeretéből származó stratégiai előnyt **Szun Vu** a következőképpen fogalmazta meg a **Szun Ce (Szun útja)** szerzőként jegyzett „**A háború művészete**” című művében:

„…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. …”

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság szerepe

A téma súlyát tekintve az **információbiztonság komplex védelmének**, irányítási rendszerének kialakításakor a biztonságtudatos viselkedés **a legfontosabb védelmi vonal, mely terület fejlesztése preventív védelmi intézkedés.**

Minden **rendszer** annyira sebezhető, sérülékeny, mind ahogy a **leggyengébb eleme**: egy információs rendszer védelmi kontrolljainak teljes körűnek, valamennyi rendszerelemre kiterjedőnek – így **a humán faktor**ra vonatkozóan is –, folyamatosnak és zártnak kell lennie.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság szerepe

A téma időszerűségét igazolják a közelmúltban a világon végig söprő **zsarolóvírus támadások**, napvilágra került, nagy rendszereket érintő **adatszivárgások**, nemzetbiztonsági **kibervédelmi eszközök és adatok kompromittálódása**, az egyre erősödő, a **kibervédelmi és támadó potenciált érintő „fegyverkezési verseny”**, illetve **a civil területen a szervezett bűnözés** megjelenése az elektronikus rendszerekkel szemben végrehajtott támadások területén.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság szerepe

„Mindig az embert kell meggyőzni arról, hogy tegyen magáért, az egészségéért még a betegséget megelőzően, így a kiberbiztonság tekintetében is magának az embernek a biztonságtudatosságát kell növelni ***az elkerülhető*** *incidensek megelőzésének érdekében.”*

Mint minden **preventív eszköz**, az információbiztonság tudatosság képzés hatékonyabb és **olcsóbb mint** az incidenst követő **korrektív eszközök, eljárások, folyamatok.**

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztésének alapjai – egyfajta megközelítés

Szövetséges Egyesített Információs Műveleti Doktrína (Allied Join Doctrine for Information Operations) AJP-3.10 NATO dokumentációja:

- ✓ Psychological Operations (PSYOPS) mint **lélektani műveletek**;
- ✓ Presence, Posture and Profil (PPP) mint **megjelenés, viselkedés és arculat**;
- ✓ Operations Security (OPSEC) mint **műveleti biztonság**;
- ✓ Information Seurity (INFOSEC) mint **információbiztonság**;
- ✓ Key Leader Engagement (KLE) mint **kulcsfontosságú vezetőkkel kapcsolatos tevékenység;**
- ✓ Computer Network Operations (CNO) mint **számítógép hálózati műveletek**;
- ✓ Civil-Military Cooperation (CIMIC) mint **civil- katonai együttműködés.**

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztésének alapjai

Az információbiztonsági kockázatok kezelése részben az érintett kockázathoz tartozó **fizikai, adminisztratív vagy logikai kontrollok bevezetése**, részben a megjelölt műveleti alkalmazási területek által érintettek biztonságtudatossági képzése útján valósítható meg. A **képzési rendszer kidolgozásánál** az egyes műveleti területek **célcsoportjai részére** – tekintettel az eltérő fenyegetésekre – **eltérő formai és tartalmi elemeket, módszereket szükséges használni.**

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztésének alapjai

Innen már csak egy logikai lépés, hogy a **civil területen egy vállalatban dolgozók vonatkozásában az eltérő munkakörök, szerepkörök**, illetve az információfeldolgozás és hozzáférés módja, valamint a feldolgozott információk minősítése/besorolása alapján leképezésre kerüljön az információbiztonság tudatosság fejlesztésénél **módszertani, formai és tartalmi szempontból diverzifikált képzések kialakítása.**

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztésének alapjai

Érdekes adat:

Magyarországi általános iskolai **informatikai képzéssel** egy tanuló mindösszesen **180 órát tölt el**, ami a teljes **minimális órakeret kevesebb mint 2%-a**.

A közép és felsőfokú oktatás is hasonlóan elhanyagolja az IBT fejlesztét.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztésének alapjai

Az alapok hiányában nagyon fontos, hogy legyen egy egységes, alapozó jellegű, általános információbiztonság tudatosság tartalmi elem, mely vagy az egyes területek diverzifikált képzéseibe kerüljenek beépítésre, vagy pedig e**gységes módon egy minden felhasználó részére kötelező alapképzési kurzust/modult kell kialakítani.**

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztésének alapjai

2015-ben kiadott „Digital Security Risk Management for Economic and Social Prosperity” OECD kiadványban általános irányelvek szintjén megmaradt a tudatosság alapelve a következő formában: „*Tudatosság, szakértelem, képességfejlesztés*”, a felvezető szöveg pedig a következő: „*Minden érintettnek meg kell ismernie a digitális biztonságot fenyegető kockázatokat, és kezelésének módjait*”

A megközelítés a 13 év alatt a biztonság szükségszerűsége irányából a kockázat menedzsment irányába lépett, azonban **a felhasználói tudatosság súlya továbbra is kiemelt.**

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztésének alapjai

Személyes tapasztalataimra támaszkodva meg tudom erősíteni: a **legsúlyosabb információbiztonsági incidensünk** egységes, megfelelően konfigurált piacvezető végponti védelmi szoftver mellett következett be, amit a **felhasználónak nem megfelelő biztonságtudatos magatartása okozott.**

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – nagyvállalati gyakorlat

A felhasználók, illetve egyéb érintettek információbiztonságot érintő **képzés elemei** az egyes kontrollok, fenyegetések, illetve a védelem irányítási és architektúrális elemei között **szétszórva jelennek meg**.

Nem tartom helyesnek ezt a fajta megközelítést, a terület fontosságát tekintve egy **külön egységes blokkban szervezve kell megjelennie a képzési rendszernek**, hiszen az információbiztonságot meghatározó többi védelmi kontrollhoz hasonlóan a képzés folyamatos fejlesztést igényel.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – Social engineering jelenség

Kevin D. Mitnick határozta meg, mely magyarul, nem szó szerinti fordítással azt jelenti, hogy a **social engineering során a támadó az áldozat emberi tulajdonságait kihasználva**, befolyásolás, meggyőzés, manipuláció, megtévesztés útján **szerez meg információt technológia felhasználásával vagy anélkül.**

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – Social engineering jelenség

A **social engineering téma beépítése** javasolt a **vezetők, erőforrásgazdák képzésébe**, ugyanis jelentősen hozzájárulna egy social engineering támadás meghiúsításához: megfelelő ismereteket nyújtana a felhasználónak az árulkodó jelek elrejtésére és azok felismerésére a támadó tevékenységében, testbeszédében.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – Social engineering jelenség

Adathalász támadással összefüggő pszichológiai manipulációs eszköztár kibontása, illetve a védekezési technikák ismertetése véleményem szerint nagyban hozzájárul egy **általános, minden felhasználóra kiterjesztett információbiztonság tudatosság fejlesztését célzó alapképzés sikeréhez.**

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – lehatárolás 1

Valamennyi információs rendszert használó munkatárs vegyen részt a képzésen, ez az alap, az egységes **alapképzés**;

Valamennyi erőforrás, illetve folyamatgazda részére az alapképzésen túl, kiegészítő oktatás útján szükséges képzéseket tartani, melyek során a vezetői információbiztonság irányában történő elkötelezettség és támogató szerep erősítését kell elérni:

- ✓ a **minőségszemélet**,
- ✓ az informatikai biztonság, **biztonságszemlélet**
- ✓ a kapcsolódó **szabályozók ismerete**,
- ✓ az incidens, katasztrófa, ügymenet folytonosságot érintő területeken **elvárt magatartás**;

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – lehatárolás 2

Valamennyi, **információbiztonság szempontjából operatív feladatellátással érintett munkatárs** részére az alapképzésen túl, kiegészítő oktatás kialakítása szükséges, az alábbi – operatív, támogató és véleményformáló – képesség fejlesztését megcélozva:

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

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere - Forma

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*]

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – Alapképzés

- ✓ Bevezető;
- ✓ Alapfogalmak ismertetése;
- ✓ Szabályozási környezet ismertetése;
- ✓ Fenyegetettségek, fenyegetések bemutatása, referenciamodell alkalmazásával;
- ✓ Social engineering témakör;
- ✓ Védelem kialakítása.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – Alapképzés – kiegészítő jelenléti konzultáció

- A **fenyegetettség bemutatása** tömbhöz kapcsolódó gyakorlati ismeretek, esettanulmányok, leírások, a hallgatóság bevonásával végrehajtott konzultációk;
- A **social engineering** témakörhöz kapcsolódóan a téma támadó oldali szemszögből történő bemutatása, rávilágítva az áldozati szerep elkerülésének gyakorlati módszereire:
  - hogyan ismerjük fel, hogy manipulálni próbálnak,
  - hogyan ne legyünk áldozatok,
  - teendők social engineering támadás esetén.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – Információbiztonság operatív szereplői részére

- **Szabályozási környezet**: 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**: eljárásrendek ismertetése fizikai biztonság, informatikai üzemeltetés és incidenskezelés területén Gyakorlati megközelítésben, példákkal, esettanulmányokkal színesítve;
- **Kommunikáció, stresszkezelés**: operatív feladatellátás során elvárt viselkedés, asszertív kommunikáció, stresszel járó szituációk kezelése.
- **Social engineering**: kockázatként megjelenő humán és számítógép alapú technikák gyakorlati példákon, esettanulmányokon keresztüli megközelítése.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – Információbiztonság operatív szereplői részére 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).
- ✓ Szabályozókkal, szabályozási környezettel kapcsolatos **feladatkataszter, RACI felelősségi tábla gyakorlati bemutatása**.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – Vezetői e-learning kurzus

- **Szabályozási környezet:** a szervezet és adatvagyon védelmének szemszögéből bemutatva az egyes szabályozó elemeket (jogszabályok, szabványok, ajánlások, információbiztonsági, adatvédelmi, minősített adatkezelést érintő kormánymegbízotti utasítások, a biztonsági vezető által kiadott 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:
  - az 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.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – 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.

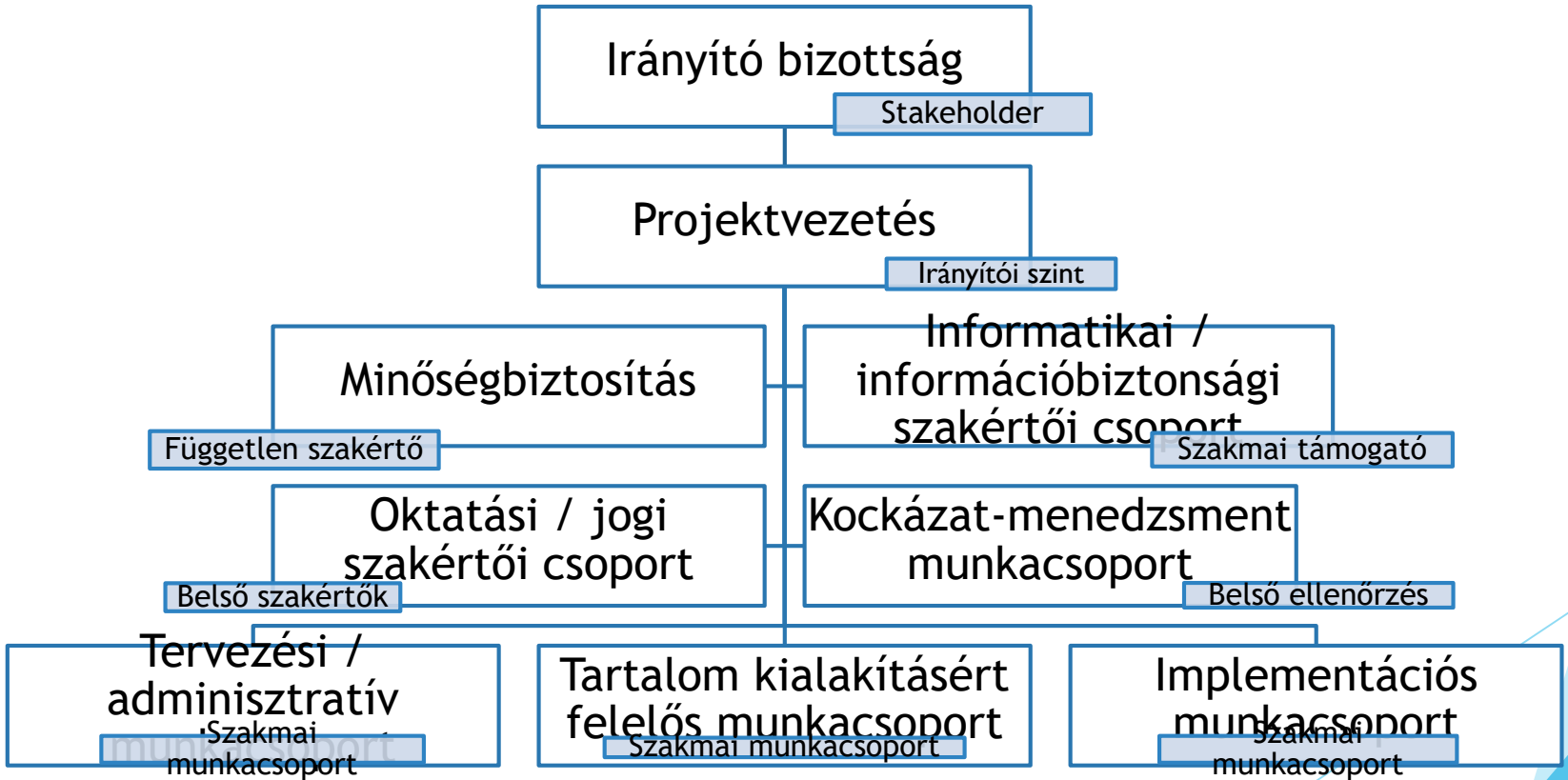
HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – Számonkérés

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

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság Képzési rendszere – Képzés „Projektszervezete”



HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztésének további lehetőségei

- **Rendszeres hírlevél** formájában, munkahelyen és a személyes térben is értelmezhető információbiztonsági kérdésekben információ közlés, tömör és közérthető formában;
- A rendkívüli, információbiztonságot érintő események kapcsán **soron kívüli tájékoztató levél** kiküldése valamennyi érintett felhasználó részére.
- Rendszereket érintő változások közlése céljából vezetői és felhasználói kört érintve **normatív utasítások, tájékoztatók kiadása**, a megismerés tényének igazolása és bizonyítása mellett.
- A Kormányhivatal hivatalos oldalán a szabadon terjeszthető besorolású információkat felhasználva, **információbiztonsági tematikájú aloldal** kialakítása, hír blokkal, eseménynaptárral, illetve a korábbi hírlevelek, tájékoztatók anyagának kivonatával.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztésének további lehetőségei

- Az **információbiztonság felhasználói tudatosság szintjének erősítésének, illetve a kapcsolódó normakövető képesség ellenőrzését célzó kampányok** kialakítása az információbiztonság tudatosság felhasználói szinten megjelenő elemeire, mint például tiszta asztal, tiszta képernyő, jelszó szabályok, felhasználói ismeretek;
- **Információbiztonsági szakmai nap** tartása nagyobb létszámú szervezeti egységek saját telephelyein, **helyben** = saját munkahelyén, a felhasználó szemszögéből saját környezetben kerüljön megvalósításra. Eredménye a kötetlenebb hangnemben, általános információbiztonsági tematikával, vagy egy adott – aktuális - téma köré szervezett, kézzelfogható közelségbe került interaktív tematikus előadás.
- **Információbiztonság tudatossággal összefüggő versenyek, vetélkedők** megtartása, lehetőség szerint valamilyen kézzel fogható nyereménnyel, elismerő oklevéllel.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztésének további lehetőségei

- Informatikai üzemeltetésben és a biztonsági feladatellátásban részt vevők részéről **felhasználóbarát és asszertív kommunikáció képességét fejlesztő tréningek** kialakítása, a kompetencia elsajátításához szükséges értekezletek, megbeszélések tartása.
- **Informatikai üzemeltetésben és a biztonsági feladatellátásban részt vevők részére rendszeres értekezlet**, megbeszélés a területet érintő változásokról, megfelelőségek biztosításáról, az egyes rendszerelemek üzemeltetésével összefüggésben kiscsoportos megbeszélések, kampányok kialakítása.
- A Kormányhivatal, illetve a kapcsolódó szervezetek által szervezett rendezvényeken az információbiztonsági területet, a tudatosság fejlesztését erősítő jelenlét **önálló stand, napirendi pont, workshop elem alkalmazása**.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

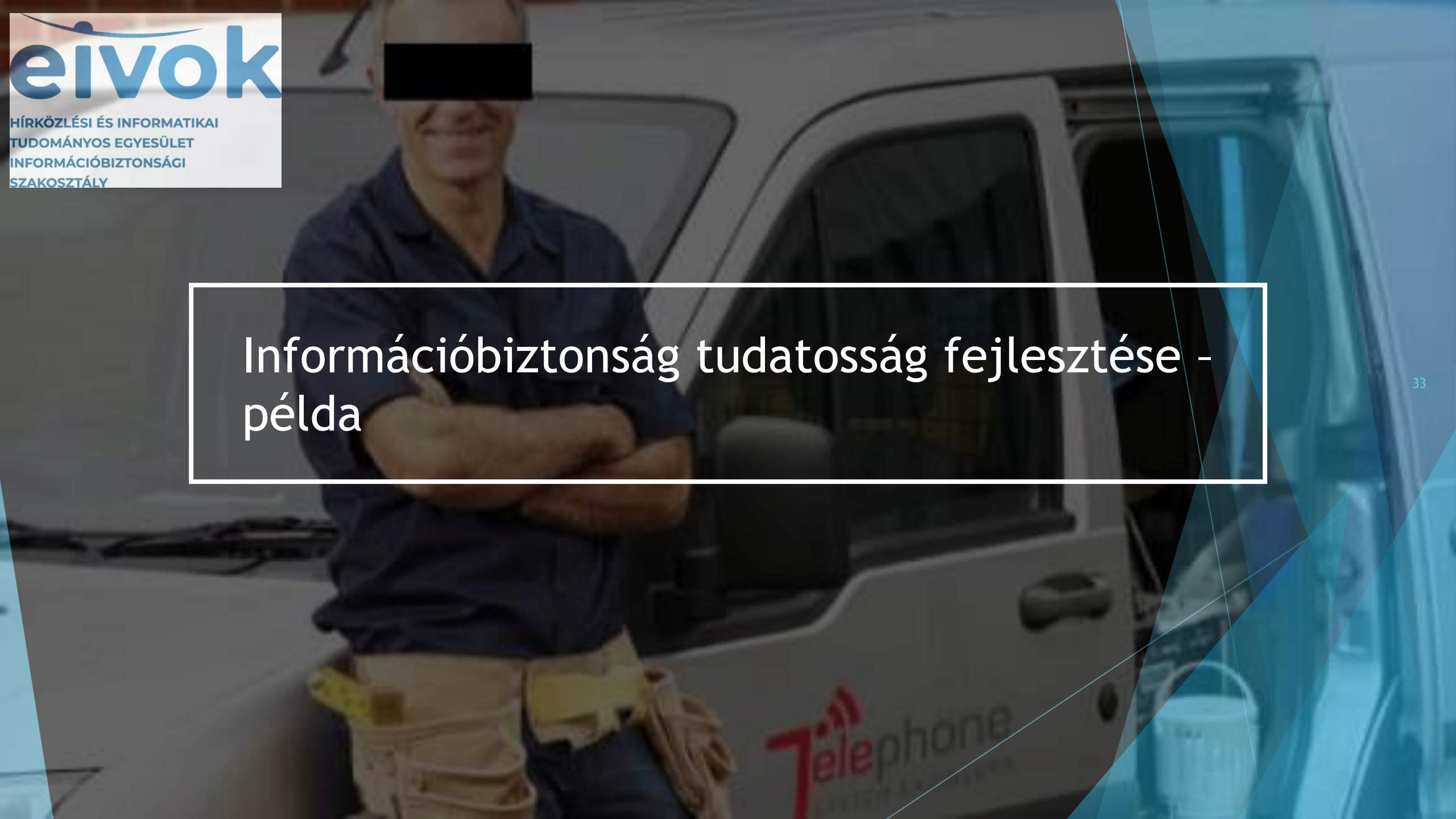
Információbiztonság tudatosság fejlesztésének Szinergikus hatásai

- 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.**

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztésének további hatásai

- 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.**



HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

Információbiztonság tudatosság fejlesztése - példa

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

„Minden háború az első csata előtti utolsó pillanatban dől el.” – Szun Vu

Köszönöm szépen a megtisztelő figyelmüket

Bubán Márton

EIVOK-6. Információbiztonsági Szakmai Fórum

2018.10.04