Biztonsági kultúra kialakítása

Az alábbi kérdésekre adott válaszok határozzák meg, hogy milyen területen és mit szükséges fejleszteni.

1. Tudják-e, indokoltnak tartják-e jogaikat, kötelezettségeiket?
2. Tevékenységük során azok szerint járnak-e el?
3. Felismerik-e a védelmi intézkedések szükségességét, van-e veszélyérzetük?
4. Felismerik-e, és elítélik-e azokat, akik a biztonsági szabályokat megsértik, a védelmi intézkedéseket nem rendeltetésszerűen hajtják végre?
5. Vállalják, hogy hatást gyakorolnak a biztonsági követelményeket tudatosan vagy véletlenül, emberi gyengeségük miatt, részben illetve egészében megsértő kollégákra?
6. Felismerik-e, akarják-e felismerni a nem erkölcsös, etikus magatartást tanúsítókat?
7. Biztonsági tudatosságuk révén konstruktív részesévé válnak-e a szervezeti egység, csoport szubkultúrájának?

Milyen a biztonságtudatos szervezet?

A szervezet biztonságáért vállalt felelősség, a szervezet vezetése által meghatározott biztonsági szintnek, mint követelménynek elfogadása és a hiánya következményeinek elismerése, valamint a biztonsági szempontból erkölcsös, etikus magatartási kultúra együttesen jellemzi a biztonság tudatos szervezetet.

Egy szervezetnél akkor jó a biztonsági kultúra, ha a munkatársak ismerik jogaikat és kötelezettségeiket, és érvényesítik is azokat.

Azoknak a munkatársaknak, akik tudatlanságból, hanyagságból, vagy szándékosan nem biztonságtudatosan viselkednek, ismételt biztonságtudatossági oktatáson kell részt venniük, illetve el is marasztalhatják őket. **A biztonsági kultúrát** tehát **az egyének biztonságtudatos magatartása alakítja ki, ahol kialakult, ott a munkatársak tudják, mi veszélyeztet(het)i a biztonságot, és ennek megfelelően cselekszenek is.**

Az egészséges veszélyérzetnél annyiban különbözik a biztonságtudatosság, hogy nem csak felismerjük, hogy a biztonsági elvárásoktól eltérő viselkedés veszélybe sorolhat minket, vagy a szervezetet, hanem azt is, hogy ilyen helyzetben mit tegyünk, és mit ne tegyünk.

A biztonságtudatosságra külső (pl. jogszabályok, szabványok, politikai hatások, piaci hatások, természeti hatások, egyének környezetének) és belső tényezők (pl.: szabályzatok, a közvetlen vezetés utasításai, humánpolitika, az ellenőrzés) egyaránt hatással vannak.

Azért fontos a vállalati kultúra részévé tenni a biztonságot, mert a szervezeti kultúra befolyásolja az egyének hovatartozás tudatát, helyzetét, szerepét a szervezetben. Tehát a biztonsági kultúra, és a szintjének fenntartása, vagy emelése önmagában is védelmi intézkedés.

A biztonságtudatosság megjelenhet vállalati szokásokban (pl. minden értekezlet után a fali táblát letöröljük), a belső kommunikációban használt nyelvezetben, és szimbólumok alkalmazásában.

A biztonságtudatosság hiányában a szervezet nem ismeri fel megfelelően a rendkívüli biztonsági eseményeket, és nem képes felmérni azok következményeit.

Alapvető módszer az, ha felkészítik a felhasználókat, a szervezet munkatársait arra, hogy felelősen, a biztonságot veszélyeztető tényezők ismeretében végezzék munkájukat. Továbbá legyenek felkészítve azoknak az eszközöknek és információs rendszereknek a használatára, amelyek szükségesek a munkájukhoz, így is csökkentve az emberi hibákból fakadó biztonsági eseményeket.
Ennek eredményességét hivatott fokozni, jelen anyag.

Biztonsági kultúra megvalósításának alapelvei

1. **Tudatosítás elve**

   Meg kell értenünk és tudatosítanunk, hogy az információs rendszerek és hálózatok hasznát csak úgy élvezhetjük, veszélyeiket csak úgy kerülhetjük el, ha a biztonsági kockázatok tudatában használjuk őket.
   Az első védelmi vonal tehát az informatikai kockázatok és a rendelkezésre álló védelmi lehetőségek tudatosítása. A kockázatok belső és külső irányból is felmerülhetnek. Ez azt jelenti, hogy egy felhasználói, vagy üzemeltetési hiba veszélyeztetheti a saját, illetve a vele kapcsolatban levő rendszerek és hálózatok biztonságát. Az integrált rendszerek megfelelő biztonsága érdekében az érintetteknek ismerniük kell a rendszerük felépítését, a hálózatokban elfoglalt helyét, és a biztonság érdekében alkalmazható intézkedéseket.

2. **Felelősség elve**

   A felhasználók, az üzemeltetők, a fejlesztők és a tulajdonosok is felelősek az információs rendszerek és hálózatok biztonságáért. A rendszerek biztonsága függ a velük összeköttetésben levő helyi és globális rendszerek biztonságától. Ahhoz, hogy a biztonságot fenn tudjuk tartani, minden érintettnek tudatában kell lennie saját felelősségével, és ezt számon kell tudni rajta kérni.
   Minden szervezetnek rendszeresen felül kell vizsgálnia saját szabályzatait, gyakorlatait, intézkedéseit és eljárásait, és értékelnie kell, hogy ezek megfelelőek-e. Minden érintettnek, aki részt vesz informatikai termékek és szolgáltatások fejlesztésében, tervezésében és szállításában, foglalkoznia kell a rendszerek és hálózatok biztonságával és a szükséges tájékoztatást időben meg kell tennie. Ennek eredményeként a felhasználók jobban megértik a termékek és szolgáltatások biztonsági vonatkozásait és a saját felelősségüket a biztonsággal kapcsolatban.

3. **Válaszintézkedések elve**

   Az érintetteknek kellő időben, egymással együttműködve kell a váratlan biztonsági eseményeket megelőzni, észlelni, illetve az ezekre vonatkozó megfelelő válaszintézkedések megtenni.
   Felismerve az információs rendszerek és hálózatok összekapcsolódását, és a gyors és széleskörű károkozás lehetőségét, az érintetteknek időben és együttműködve kell a

váratlan biztonsági eseményeket kezelni. Szükség szerint meg kell osztaniuk egymással a fenyegetésekkel és sebezhetőségekkel kapcsolatos információkat, és gyors és hatékony eljárásokat kell alkalmazniuk, hogy együttműködve megelőzzék, észleljék, illetve reagáljanak a váratlan biztonsági eseményekre. Ahol lehetséges, ez akár határokon keresztüli információcserével és együttműködéssel is járhat.

4. Az etika elve

Az érintetteknek tiszteletben kell tartaniuk mások jogos érdekeit.

Tekintettel arra, hogy az információs rendszerek és hálózatok alkalmazása átszövi a társadalmunkat, az egyéneknek fel kell ismerniük, hogy cselekedeteik vagy azok hiánya adott esetben káros hatással is lehetnek a többi felhasználóra. Az etikus viselkedés ezért létfontosságú, az érintetteknek törekedniük kell arra, hogy a jó gyakorlatokat kialakítsák és alkalmazzák, a biztonság igényét elfogadják, és mások jogos érdekeit tiszteljék.

5. A demokrácia elve

Az információs rendszerek és hálózatok biztonságát megvalósító megoldásoknak a demokratikus társadalmak alapvető értékeivel összeférhetőnek kell lenniük.

A gondolatok és eszmék cseréjének szabadságát, az információ szabad áramlását, a személyes adatok megfelelő védelmét, a nyitottságot és az átláthatóságot indokolatlan mértékben nem szabad korlátozni.

6. A kockázatfelmérés elve

A biztonság tervezése és megvalósítása során a releváns lényeges kockázatokat fel kell mérni.

A kockázatfelmérés azonosítja a fenyegetéseket és a sebezhetőségeket, kitérve a legfőbb belső és külső tényezőkre, úgymint a technológia, a fizikai és emberi tényezők, politikai irányelvek és harmadik személy által nyújtott biztonsági szolgáltatások. A kockázatfelmérés lehetővé teszi az elfogadható szervezeti kockázati szint meghatározását, és segítséget nyújt az információs rendszerek és hálózatok biztonságát fenntartó megfelelő szabályozások kialakításában a megvédendő információ jellegével és fontosságával arányban. Tekintettel az információs rendszerek összekapcsolására, a kockázatfelmérésnek ki kell térni a másoktól származó, vagy a mások részére okozható hatásokra.

7. **Biztonságtervezés és végrehajtás elve**

Az érintetteknek a biztonságot az információs rendszerek és hálózatok kialakítása során lényeges szempontként kell kezelni, és megvalósítani.
A rendszereket, hálózatokat és irányelveket az optimális biztonság megvalósítására kell megtervezni, alkalmazni és koordinálni. Megfelelő óvintézkedéseket kell tervezni és elfogadni annak érdekében, hogy az azonosított fenyegetésekből és sebezhetőségekből származó potenciális károkat elkerüljék, vagy csökkentsék. A szervezet rendszereiben és hálózataiban található információ értékével arányos műszaki, és nem műszaki óvintézkedésekre van szükség. A biztonságot az összes termék, szolgáltatás, rendszer és hálózat alapvető elemévé, valamint a rendszertervezés és az architektúra szerves részévé kell tenni. Az átlagos felhasználók számára ez leginkább saját igényeik meghatározására, a termékek és szolgáltatások kiválasztására terjed ki.

8. **Biztonságmenedzsment elve**

Az érintetteknek minden szempontra kiterjedő módon kell a biztonság-menedzsment feladatokat végezniük.
A biztonságmenedzsmentnek kockázatfelmérésen kell alapulnia, felölelve az érintettek tevékenységének és működésének minden vonatkozását. A rendkívüli események megelőzésére, feltárására, és velük kapcsolatos válaszintézkedésekre, rendszer helyreállításra, karbantartásra, felülvizsgálatra és ellenőrzésre vonatkozó előremutató válaszokat kell adnia a kialakuló fenyegetésekre vonatkozóan. Az információs rendszerek és hálózatok biztonságával kapcsolatos irányelveket, gyakorlatokat, intézkedéseket és eljárásokat össze kell hangolni az összefüggő biztonsági rendszer kialakítása érdekében.
A biztonságmenedzsmentre vonatkozó követelmények függenek az érintettség szintjétől, az érintett szerepétől, a szóban forgó kockázatoktól és rendszerkövetelményektől.

9. **Újraértékelés elve**

Az érintetteknek az információs rendszerek és hálózatok biztonságát felül kell vizsgálniuk és újra kell értékelniük. A biztonsági irányelvekben, gyakorlatokban, intézkedésekben és eljárásokban szükséges módosításokat el kell végezniük.
Folyamatosan jelennek meg új és változó fenyegetések, és sebezhetőségek. Az érintetteknek a biztonság minden aspektusát folyamatosan felül kell vizsgálniuk, át kell értékelniük és változtatniuk kell, hogy a felmerülő kockázatokat kezelhessék.