Vállalkozói digitális kompetenciák fejlesztése

Biztonsághoz kapcsolódó kompetenciák a digitális térben

SZÉCHENYI 2020
MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Szociális Alap
BEFEKTETÉS A JÖVŐBE

Tartalomjegyzék

A vállalkozások folyamatosan keresik azokat a lehetőségeket, melyekkel gyorsabban és hatékonyabban menedzselhetik folyamataikat. A 21. században ehhez a legtöbb fegyvert a digitális eszközök biztosítják. Ráadásul az Európai Bizottság felmérése szerint a ***munkakörök több mint 90%-a esetén szükség lesz digitális kompetenciákra.***

Mindezek tükrében az e-book célja, hogy segítse a vállalkozói digitális kompetenciák fejlesztését. A program tematikája úgy került összeállításra, hogy összhangban legyen az Európai Bizottság által meghatározott DigComp kompetencia területekkel.

A vállalati adat, mint érték a 21. században

A vállalkozások működtetése kapcsán az elmúlt években jelentősen megváltozott az adatvagyon megítélése, az információk értékelése. Gondoljunk csak bele, hogy melyik vállalkozás tudna gond nélkül tovább működni, ha holnap eltűnnének az adatai a számítógépeiről, okostelefonjairól, szervereiről vagy a CRM rendszeréből. Ha ellopják a laptopunkat, akkor ma már a rajta lévő adatok többet érnek, mint maga az eszköz.

Új korszakba léptünk tehát a vállalkozások információbiztonsága kapcsán.

Most nézzünk meg egy ehhez a témához kapcsolódó videót!

Minél több feladatot bízunk a szoftverekre, alkalmazásokra, annál nagyobb szerepet kap az adatok és információk védelme. Hiszen komplett rendszerek automatizálása azt is eredményezheti, hogy azok felett rosszindulatú elkövetők, hackerek, kiberbűnözők a teljes kontrolt át tudják venni. Vállalkozásként tehát folyamatosan mérlegelnünk kell, hogy a hatékonyság növelése együtt jár-e az IT biztonsági kockázatok növelésével? Milyen felelősége van a vállalkozás menedzsmentjének a kollégák felkészítése kapcsán, és milyen felelősége van az egyes munkavállalóknak a mindennapi feladatok elvégzése során. Hiszen egy vírus vagy rosszindulatú program a vállalat teljes működését le tudja állítani, és pénzügyi, illetve reputációs károkat tud okozni. Fontos tehát, hogy a jövő munkavállalóit folyamatosan felkészítsük az újabb és újabb IT biztonsági veszélyekre.

Felkészültség és vállalati kultúra

Az Európai Bizottság által meghatározott digitális kompetenciák közül (Európai Bizottság, 2017) az IT biztonság kapcsán van a munkavállalóknak talán a legnagyobb felelősége. Éppen ezért kiemelt vezetői feladat lett és lesz a jövőben, hogy az IT biztonsági kérdésekről beszéljünk és ezeket a készségeket folyamatosan, közösen fejlesszük. Nézzünk most néhány példát a különböző szintekhez kapcsolódóan.

Alapszint: A munkavállaló képes meghatározni egyszerű módszereket digitális eszközei (pl. laptop, okostelefon, tablet) megóvására. Képesek továbbá megkülönböztetni egyszerű kockázatokat és veszélyeket az online világban, illetve kiválasztani egyszerű biztonsági lépéseket, intézkedéseket. Mindez azt is jelenti a mindennapi feladatok elvégzése során, hogy munkavállalóként figyelünk a jelszavak, pin és belépő kódok védelmére, és meghatározott időközönként cseréljük őket.

Középszint: A munkavállaló képes önállóan frissíteni a vírusvédelmi szoftvereket. Képes azonosítani, hogy mely levelek érkeztek megbízhatatlan forrásból, és rejtenek IT biztonsági kockázatot. Tudja, mi a teendő, ha IT biztonsági támadásra utaló jeleket észlel.

Felsőszint: A munkavállaó képes a veszélyeket megfelelő intézkedésekkel (pl. az adatvédelmi beállítások módosításával) kezelni. Fontos számára, hogy a többi kollégával is megossza az IT biztonsági incidensek tapasztalatait, és felismeri, hogy az adatok és információk védelme a vállalati kultúra része kell, hogy legyen.

Fontos, hogy a munkavállalók felismerjék, hogy mely tevékenységek esetében van nekik egyéni felelőségük,

---

és mely kérdésekben kell segítséget nyújtania egy szakértő kollégának (pl. rendszergazdának, vagy IT biztonsági szakértőnek). Ezeket a feladatokat most tanulja, ismeri meg a legtöbb hazai vállalkozás, ezért fontos, hogy ezen témák egyeztetésre is teret adjunk, ne hagyjuk magukra a kollégákat.

Támadási felületek

A korábbi modulokban bemutatott témakörök (online kommunikáció, digitális tartalmak) kapcsán számos esetben merülhetnek fel IT biztonsági kérdések. Nem mindegy, hogy a videós megbeszélésekre használt szoftverünket milyen könnyű feltörni kívülről? Vajon az általunk létrehozott oktató videókat a YouTube privát csatornánkon biztonságban vannak? Mekkora az esélye, hogy a konkurens vállalkozás által küldött e-mail tartalmazhat olyan programot, ami ellopja adatainkat?

Nézzünk meg most néhány fontos alapfogalmat a témakörhöz kapcsolódóan!

A munkavállalók felelősége

Egyre fontosabb a vállalkozásunk informatikai, adatvédelmi szabályainak ismerete, hiszen ma már a munkavállalók ugyanúgy felelősek az IT biztonsági szabályok betartásáért, mint ahogy a munkavédelmi, szabályokért. Egyre gyakoribb kérdés, hogy a munkavállalóknak milyen esetekben van jelentéstételi kötelezettségük, ha valamilyen támadásra utaló dolgot észlelnek az informatikai rendszerek kapcsán.

IT biztonsági incidensek: olyan váratlan jelenségek, amely károsan hatnak a vállalkozás által használt digitális eszközökre, szoftverekre, alkalmazásokra, illetve a tárolt információkra, adatokra. Ezek az események kapcsolódhatnak konkrét fájlokhoz, de érinthetik a vállalkozás komplex rendszereit is (pl. honlap, levelező rendszer, CRM, ERP)

Online csatornákon érkező támadások: Az egyik leggyakoribb támadási forma, amikor valaki egy fiktív, hamisított e-mail címen keresztül veszi fel velünk a kapcsolatot. Mi ilyenkor nem vesszük észre, hogy az adott e-mail cím nem teljesen egyezik a partnerünk korábbi, megszokott e-mail címével. Történhet mindez például adathalászat céljából. Szerencsére ma

már viszonylag jól kiszűrik a kéretlen, spam leveleket a vállalati rendszerek, de az már a mi felelősségünk, hogy az érzelmeinkre építő hoax vagy láncleveleket tovább küldjük-e.

Adatok védelmével érintett vállalati területek

Ha szeretnénk a vállalkozásunk IT biztonsági kérdéseit kezelni, akkor az alábbi csoportosítás segítséget nyújthat nekünk a teendőink rendszerezése során:

- Jelszavak;
- Levelezés, külső kommunikációs csatornák;
- Adatszivárgás;
- Vírusvédelem;

PIN kódok és jelszavak tengere

A vállalati feladatainkhoz ma már legalább egy tucat belépési azonosítót, jelszót és PIN kódot kell folyamatosan tudnunk. Mindez óriási teher a munkavállalókon, és elég egy kisebb vis maior eset, és máris könnyen megszeghetjük a legalapvetőbb IT biztonsági szabályokat is. A következőkben bemutatunk néhány tipikus munkavállalói hibát:

- Emberi dolog, és bizony előfordul, hogy amikor lebetegszünk, akkor felhívjuk egy kollégánkat, és megkérjük, hogy a belépési azonosítónkkal csatlakozzon különböző vállalati IT rendszerekhez, és segítsen nekünk elvégezni egy-két feladatot, lezárni néhány munkafolyamatot. Mindez óriási IT biztonsági kockázattal jár, és elég, ha egy ilyen üzenet illetéktelen kezekbe kerül.

- Semmiképp se telepítsünk játékokat, programokat engedély nélkül a munkahelyi digitális eszközünkre. Ma már hetente jelennek meg olyan listák, melyek adathalász, rosszindulatú applikációkat sorolnak fel. Sok esetben akár a családtagjaink, gyerekünk által telepített játékokon keresztül is érkezhetnek ilyen támadások, ezért fontos, hogy ők ne férjenek hozzá a vállalati eszközökhöz.

- Nagyon fontos, hogy soha ne hagyjuk az IT eszközeinket bejelentkezve őrizetlenül, akár egy kávézóban, vagy egy partnerünk irodájában. Ha ilyen esetekben valaki hozzáfér a vállalati adatokhoz, akkor bennünket fog komoly felelősség terhelni.

Milyen a jó jelszó?

Az informatikai rendszerekben használt jelszavaink esetében vannak olyan szabályok, melyeket érdemes figyelembe venni, mikor létrehozzuk őket. A kihívás abban van, hogy miként olyan jelszavakat kreálni, melyeket meg tudunk jegyezni, ugyanakkor elég bonyolultak ahhoz, hogy ne lehessen őket könnyen feltörni. Nézzük meg ennek kapcsán milyen szabályokat érdemes betartani:

- a jelszavunk legyen kellően hosszú (jellemzően 8 karakter),
- az ABC kis- és nagybetűinek, számok és speciális karakterek kombinációiból álljon.

Levelezés, mint támadási felület

Az ismeretlen személytől származó, általunk nem kért, esetenként tárgy nélkül érkező elektronikus levelek nagy valószínűséggel:

- tartalmaznak az informatikai rendszerre és az adatvagyonra káros hatást kifejtő, rosszindulatú programkódokat.
- Az ilyen e-maileket spam-nek (kéretlen levélnek) kell tekintenünk, és azokat biztonsági okokból azonnal törölnünk kell.

Adatszivárgási kérdések

A vállalat vagyonába nemcsak a pénzügyi tételek tartoznak bele, hanem az adatok és információk értéke is! Hiszen egy új termék jellemzői, vagy egy tervezett beruházáshoz kapcsolódó információk jelentős értéket jelentenek például a konkurenciának. Éppen ezért egyre nagyobb teret kap az adatszivárgás megakadályozása, a munkavállalók ehhez kapcsolódó felelős viselkedése.

Mindig gondoljuk tehát végig, hogy azok az információk, amelyek egy e-mailben vagy annak csatolmányában vannak, vagy elhangzanak egy tárgyaláson, vajon kerülhetnek-e illetéktelen kezekbe?

Vírusvédelem

A számítógépes vírusokra ma már számos definíció létezik, de alapvetően kisméretű, önmaguk sokszorozására és terjesztésére képes számítógépes szoftverekre kell gondolnunk. Az a funkciójuk, hogy az egyik számítógépről a másikra terjedjenek és beleavatkozzanak a vállalti rendszereink működésébe. A vírusirtó cégek laboratóriumokat tartanak fenn szerte a világon, állandóan figyelik a világhálót, és úgynevezett „mézes madzagokat", víruscsapdákat működtetnek, hogy új vírusokat találjanak. Amint egy új fennakad, és veszélyesnek ítélik, akkor megállapítják a vírus jellemzőit, típusát, és ennek alapján már blokkolni tudják a felfedezett vírusokat.

Mit tesznek a vírusok?

- A számítógépen található adatokat, sőt esetleg a teljes merevlemez tartalmát is törölhetik;
- Lelassíthatják az internetkapcsolatot;
- Lehetővé teszik a számítógép távolról történő, észrevehetetlen irányítását, miközben az így végzett tevékenységek elkövetője látszólag a jogosult felhasználó.

Érdemes tehát ezekben a kérdésekben óvatosnak lennünk, és ha bármilyen szokatlan dolgot tapasztalunk, akkor azt rögtön egyeztetni szakértővel.

A menedzsment és a munkavállalók felelőssége az IT biztonsági keretek biztosítása során

Ma már nemcsak vezetőként, hanem munkavállalóként is kötelességünk védeni a vállalat információs vagyonát és felelősek vagyunk a hozzánk rendelt informatikai eszközök megfelelő használatáért.

Nézzük meg a következőkben, hogy melyek azok a tevékenységek, szituációk, melyek gyakoriak a vállalati életben és érdemes árgus szemmel figyelnünk:

- Nagyon veszélyes ismeretlen eredetű hordozható eszközt, háttértárolót a vállalati munkaállomásra csatlakoztatni. Például ilyen lehet egy talált pendrive;
- Nem javasolt idegen, ismeretlen wi-fi hálózatra a vállalati hordozható eszközzel kapcsolódni (pl. kávézóban, benzinkúton).
- Kockázatos munkavállalóként egy másik dolgozó megszemélyesítése, vagyis az illető azonosítójával és jelszavával való munkavégzés, akár ideiglenesen is;
- Nem javasolt a munkaállomására bármilyen szoftvert telepíteni előzetes egyeztetés nélkül;
- Tilos a mobileszközöket nyilvános helyen felügyelet nélkül hagyni;

Mi az a phising (adathalászat)?

A hackerek és kiberbűnözők módszerei évről évre finomodnak, de azért érdemes néhány alapvető technikát, fogalmat megismernünk. A phising lényege a horgászathoz hasonlóan, hogy

- Valaki úgy szerzi meg a felhasználó belépési adatait, jelszavait, hogy azt maga a felhasználó adja meg (horogra akad).
- A phishing-támadás általában egy e-mailben történő megkereséssel kezdődik, a csalók spam-ként küldik ki felhívásukat (sok csalit bedobnak).
- Ebben arra próbálják rávenni a címzetteket, hogy látogassanak el az általuk üzemeltetett honlapokra, és ott adják meg személyes vagy banki adataikat.

Mire figyeljünk a vírusok kapcsán?

A vállalati eszközeink használata során előfordulhat, hogy szokatlan, korábban nem tapasztalt dolgokat veszünk észre. Ha ilyesmi történik, akkor gyanakodhatunk arra is, hogy támadás alatt állnak rendszereink.

A következőkben összeszedtünk néhány olyan árulkodó jelre, melyekre érdemes különösen odafigyelni:

1. Fokozottan figyeljünk, ha a számítógépünk minden ok nélkül újraindul, vagy a korábban jól működő operációs rendszerünk nem indul el;

2. Vírusra jelenlétére utalhat az is, ha korábban megszokott jogosultságaink hirtelen megváltoznak, például „Hozzáférés megtagadva” hibaüzenetet kapunk olyan mappára vonatkozóan, amelyet korábban gond nélkül elértünk;
3. Aggodalomra adhat okot, ha megváltoznak az böngészőnk beállításai, például más nyitóoldal jelenik meg, mint amit korábban megszoktunk.
4. Vírusra utalhat, ha folyamatosan értesítéseket kapunk ismeretlen weboldalaktól. Ezeknek a témája általában valamilyen nyereményjáték vagy pornográfia.
5. Legyünk résen, ha a számítógépünk tálcáján vagy a Start menüben számunkra ismeretlen, új ikonok jelennek meg;

Láthattuk tehát, hogy a digitális eszközök, a vállalti szoftveres megoldások számos témakörben javítják a hatékonyságunkat, és segítik a mindennapi munkánkat. Fontos viszont, hogy megértsük, ezek az eszközök folyamatosan támadásnak lehetnek kitéve, ami veszélyt jelent a vállalkozásunk adataira, működésére.

Éppen ezért ma már minden munkavállaló egyéni felelősége és feladata lett az is, hogy a fentiekben felsorolt IT biztonsági szabályokat betartsa, és vigyázzon a vállalati adatvagyonra.

Ez egy olyan tanulási folyamat, melyeken a munkavállalók világszerte most mennek keresztül, ezért érdemes minden segítséget, támogatást megadnunk a kollégáknak, és időnként kicserélni a tapasztalatainkat.