

Adatvédelemről és információbiztonságról kkv-knak: költség vagy befektetés?

A Dunaújvárosi Kereskedelmi és Iparkamara keretében létrehozott Digitális Technológiai Trendek Klub rendezvényén Mándi Zsolt, Frontend csoportvezető, vezető UX/UX designer tartott előadást a kiberbiztonság témájában.

**DUNAÚJVÁROSI
KERESKEDELMI
ÉS IPARKAMARA**

A digitális technológiákkal kapcsolatos aktuális kérdésekkel, trendekkel foglalkozó, tavaly alakult klub rendezvényét Járai Tamás, a klub vezetője nyitotta meg. Előadásai témái – így a legutóbbi is – nagyon is aktuálisak, a klub vezetése, meghívott előadói szakmai trendekbe illeszkedő, napra kész információkat adnak át. A térségben a szakterületen dolgozó vállalkozásoknak, szakembereknek ez a fórum nagy lehetőség arra, hogy egy-egy napirenden lévő témát megvitassanak. A tudásátadás, szakmai kapcsolatok által ez a fórum a helyi gazdaság fejlődése szempontjából is fontos eredményeket hozhat.

Lépést tartani a digitalizációs változásokkal, hatalmas kihívást jelent a kisebb vállalkozások számára. A közép- és nagyvállalkozások lehetőségeik alapján már átfogóbb megoldásokat valósíthatnak meg – a kiberbiztonság terén is –, számukra most éppen a NIS2 bevezetése jelenthet fokozott kihívásokat. Erről a témáról egyébként a rendezvényen csak érintőlegesen esett szó. Ugyan csak az



ötven fő foglalkoztatott, 10 millió euro éves árbevétel feletti, meghatározott területeken dolgozó cégeket érinti, azonban jó tudni, hogy az ilyen cégekkel üzleti kapcsolatot ápoló kisebb kkv-k számára is előnyt jelenthet az audit. A megrendelőnek nagyobb lehet a bizalma irántuk.

A hazai cégek eleynyésző százalékánál működnek a felmérések szerint megfelelő IT biztonsági rendszerek – kezdte előadását Mándi Zsolt. Magyarországon mintegy 900 ezer kkv működik, 3,3 millió alkalmazottat foglalkoztatnak, a fentebb említett kedvezőtlen statisztikai adatot elsősorban a nagyszámú mikro- és kisvállalkozás rontja le. Nem tudnak megfelelő informatikai szakembert foglalkoztatni, és erre nincs is szükség. Külső szakember igénybe vétele azonban indokolt, meg kell találni a költséghatékony, ugyanakkor alapvető védelmet biztosító megoldásokat. Nem egyfajta nagyobb beruházásként kell nekiindulni a biztonságtechnikai fejlesztésnek, hanem végig gondolva, lépésről lépésre.

Alapvető a leggyengébb láncszem keresése. Eláruljuk, ez maga az ember. Nem frissíti a rendszert, nincsenek megfelelő mentések, nincsenek titkosítva az adatok, gondok vannak a jelszókezeléssel, meg gondolatlanul tölt le tartalmakat, programokat, nyit meg e-maileket, bennük hivatkozásokat, ad meg adatokat nem ismerve fel az átveréseket. A saját és munkavállalóink tudatosságát, képzését szolgáló megoldások, szabályzatok már egy komoly előrelépést hozhatnak a biztonság terén. Az emberi tényező egy komoly kibérvelmi rendszer bevezetése esetén is veszélyforrást jelenthet, sőt, a hamis biztonságérzet alapján kevésbé óvatosá válhatnak a rendszerhasználók.

A mikro- és kisvállalkozások esetében a hatékony biztonsági megoldások bevezetésének gátja lehet az a szemlélet is, hogy mi nem leszünk célpontok, nálunk nincsenek ellopásra érdemes adatok. Ha pedig adatvesztés történik, károsodik a rendszerünk, blokkolják, majd megoldjuk. Azonban – ahogy a sajtóban is folyamatosan olvasható – hatalmas mértékben nő a különböző típusú kibertámadások száma. Bármely cég működésében okozhat megrázkódtatást egy adatlopás, blokkolás, hogy olyan érzékeny adatokról ne is beszéljünk, mint a banki adatok. Hatalmas növekedést mutatnak például az úgynevezett ellátási lánc elleni támadások, amikor egy megbízható

forrást jelenthet, sőt, a hamis biztonságérzet alapján kevésbé óvatosá válhatnak a rendszerhasználók.

A mikro- és kisvállalkozások esetében a hatékony biztonsági megoldások bevezetésének gátja lehet az a szemlélet is, hogy mi nem leszünk célpontok, nálunk nincsenek ellopásra érdemes adatok. Ha pedig adatvesztés történik, károsodik a rendszerünk, blokkolják, majd megoldjuk. Azonban – ahogy a sajtóban is folyamatosan olvasható – hatalmas mértékben nő a különböző típusú kibertámadások száma. Bármely cég működésében okozhat megrázkódtatást egy adatlopás, blokkolás, hogy olyan érzékeny adatokról ne is beszéljünk, mint a banki adatok. Hatalmas növekedést mutatnak például az úgynevezett ellátási lánc elleni támadások, amikor egy megbízható

nak tartott harmadik fél (pl. szoftverszállító) rendszerét fertőzik meg. Ez pedig válogatás nélkül érheti el a kisebb cégeket is. És említhetjük a botnetek rosszindulatú kialakítását is rizikóként, amiből adott esetben a felhasználó csak az adatforgalom megnövekedését, a számítógép belassulását érzékeli, de sok más veszélyt is hordoz magában.

A vállalkozásoknak arra kell törekedniük, hogy külső szolgáltatóval együttműködve felmérjék, milyen egyszeri és rendszeres költséget érdemes vállalniuk annak érdekében, hogy elkerüljék a lehetséges incidensek esetén felmerülő költségeket. Ugyanakkor az átgondolt digitális fejlesztések, a stabil működés a versenyképesség növelésére is kihatnak, növelik a bizalmat az üzleti partnerekben, sőt a munkavállalókban is.