Kerekasztal-beszélgetés a kiberbiztonságról

Nagy Konrád Ákos

10.14267/VILPOL2024.04.13

Az óbudai egyetemen kkv-k kiberbiztonsági felkészültsége, dilemmái témában került megrendezésre kerekasztal-beszélgetés Trautmann László vezetésével. A résztvevők: Pintér Róbert (Budapesti Corvinus Egyetem adjunktusa, Digiméter kutatásvezetője), Katona Gergely (Nemzeti Közszolgálati Egyetem), Kott Ferenc (MKIK Digitalizációs Kollégium vezetője, BKIK Informatikai Osztály elnöke), Márton János (Falcon ügyvezetője), Répás József (Alverad vezetője).

Az első kérdés az volt, hogy a sikeres kkv-k mennyiben támaszkodnak adatbázisaikra, menynyire tudatosan építik ezt az adatbázist, mennyire figyelnek az adatminőségre? A Digiméter felmérése szerint a hazai kkv-k kétharmada gyűjt és használ adatokat a működéséről. Ennek elsődleges eszközei az Excel adatbázisok, de szélsőséges esetekben manuális megoldások is előfordulnak, például papíron való számontartás. Tanácsadói tapasztalatok szerint az adatvezéreltség szektoronként eltérő lehet, valamint kijelenthető, hogy a vállalat méretének növekedésével a digitalizáció foka is növekszik. Felmérések és tanácsadói tapasztalatok is megerősítették, hogy a kkv-k esetében gyakori gyengeség, hogy ritkán készítenek biztonsági mentéseket, néha egy hónap is eltelhet két mentés között. Ilyen esetben egy incidens során rengeteg adat elvész, ami a termelés leállását eredményezheti.

Az aggregált Digiméter Index méri a hazai kkv-k digitalizációs szintjét 2020 óta. Ennek az átlagos értéke stagnált az elmúlt években, ami a jelentősebb fejlődés hiányát jelzi. Azonban Kott Ferenc kiemelte, hogy a hamarosan megjelenő Eurostat adatok szerint a magyar kkv-k az utolsó 4-5 évben közelítőleg 10 helyet léptek előre ERP és CRM rendszerek elterjedését illetően. Ennek egyik oka lehetett a Covid kényszerdigitalizáló hatása, a vezetők körében történt generációváltás, valamint az MKIK digitalizációs projektjén belül 15 ezer vállalkozással tudtak megegyezni és letenni egy fejlesztési tervet az asztalukra. Ez a program a vidéki településekre fókuszált, hangsúlyt helyeztek arra, hogy helyi tanácsadó vegye fel közvetlenül a kapcsolatot az adott vállalattal.

A második kérdés az volt, mennyire érzékelik a digitalizációból fakadó kockázatot a cégek? Márton Jánosnak az volt a tapasztalata, hogy oly mértékben érzékelik a kockázatot, amely már talán paranoiásnak is nevezhető. Sajnos azokkal szemben is, akik segíteni akarnak, ugyanis előfordult már, hogy informatikai tanácsadó cégek, kihasználva, hogy az ügyfeleik nem jártasok a témában, sok esetben félrevezették őket. Azonban a Covid okozta bezártság löketet adott a digitális fejlődésnek és a kkv vezetőket is nyitottabbá tette. A Digiméter riportjából is kiderül, hogy elsősorban a pénzügy területén mutatkozott előrelépés, 10-ből kilenc használ online bankolást, hat használ valamilyen applikációt.

A pénzügyi területtől még le van maradva az informatikai biztonság, pedig nem alaptalanul adhat okot félelemre ez a lemaradás. Répás József rámutatott, hogy a magyarországi vállalatokat (nem a kkv-kre korlátozva) átlagosan nagyjából 200 millió forint kár éri évente kibertámadások következtében. A Digiméter statisztikái szerint a hazai kkv-k 79%-a használ vírusirtót, 84% egyedi azonosítót (vagyis 16%-nál nincs mindenkinek külön jelszava). Többszintű jogosultsági rendszer – vagyis a vállalatban nem mindenki ugyanahhoz fér hozzá – az esetek 39%-ában fordul elő. Automatikus biztonsági mentéseket a cégek mindössze 30%-a készít.

Kisebb cégek természetesen nem mindig engedhetik meg maguknak, hogy külön személyes és külön céges informatikai eszközöket tartsanak. Ennek a keveredése komoly veszélyt jelent, ugyanis egyre inkább a magánszemélyek a támadások célpontjai. A statisztikákon is megfigyelhető, hogy a ChatGPT megjelenése kilőtte az adathalász támadások számát, egyre fejlettebbek a spam üzenetek, és a mesterséges intelligencia fejlődése nyomán már a magyar nyelvünk sem véd meg minket a külföldi támadásoktól. Nagyon fontos ilyen téren a tudatosítás, de sajnos nem csodafegyver, ugyanis ennek belső motivációból kell fakadnia, elengedhetetlen a vezetői elköteleződés. Enélkül hiába indulnak ismeretterjesztő kampányok, jellemzően nem érik el az ingerküszöböt.

Jelenleg az informatikai biztonságot célzó jogszabályok, mint a NIS 2 (EU-s jogszabály, mely fokozott védelemre kötelezi a kritikus infrastruktúrának tekintett vállalatokat) és a TISAX (autóipari szabvány) a nagyvállalatokat, illetve a beszállító kkv-kat érintik. Az a tapasztalat, hogy az ennek való megfelelést a kkv-k jellemzően a legvégső határidőig halogatják, az elvárásaikat pedig csak kipipálni törekednek, nem a szervezet számára történő értékteremtés a cél. Sok esetben nem tudják, hogy a jogszabály hatálya alá tartoznak, olyan is előfordul, hogy még alapításkor felvettek számos olyan tevékenységet, amelyet nem végeznek, de később esetleg szükség lehet rá, emiatt az előírás rájuk is vonatkozik.

A harmadik kérdés az volt, hogy látni-e hálózatosodást a kiberbiztonságra való törekvésben? A Kiberklaszter és az NKE is foglalkozik tanácsadással, tudatosítással, igyekeznek ilyen témában mindent megosztani a szektorral, de egy korlátozottabb közönséget érnek el. Az NKE nyújt automata sérülékenység-vizsgálatot, de ezt egyelőre nagyvállalatok és beszállítóik vehetik csak igénybe. Az MKIK szeretné ezt kiterjeszteni, ezért kkv-k, de akár mikrovállalkozások számára is szeretne fejleszteni ilyen jellegű szolgáltatást.

Bár a tudatosítás sajnos egy szűkebb érdeklődő kört ér el, komolyabb biztonsági incidensek a sajtó némileg hatásvadász tényked̈ésének köszönhetően nagy port kavarhatnak. Ilyen volt például a Pepco vagy a Revolut esete, amikre sokan felkapták a fejüket. A kerekasztal résztvevői fontosnak tartják az ezekhez hasonló tanulságos és figyelemfelkeltő esetek egymással való megosztását. Jó példa az UNIX vezérigazgatója, aki egy komolyabb támadási incidenssel szerzett tapasztalatait blog formájában osztotta meg. Volt olyan eset, hogy egy e-mail érkezett egy vállalathoz egy régebbi ügyféltől, hogy megváltozott a számlaszám, és máshova kéne utalni. Feltehetően az ügyfél e-mail fiókját törték fel és így csaltak ki 90 millió forintot a cégtől. Az ilyen beszámolók is kiemelik, hogy elengedhetetlenek a jól felépített folyamatok és protokollok, az ehhez hasonló tapasztalatok megosztása kulcsfontosságú a kkv szektor boldogulásához az egyre veszélyesebb kibertérben.

Összefoglalás

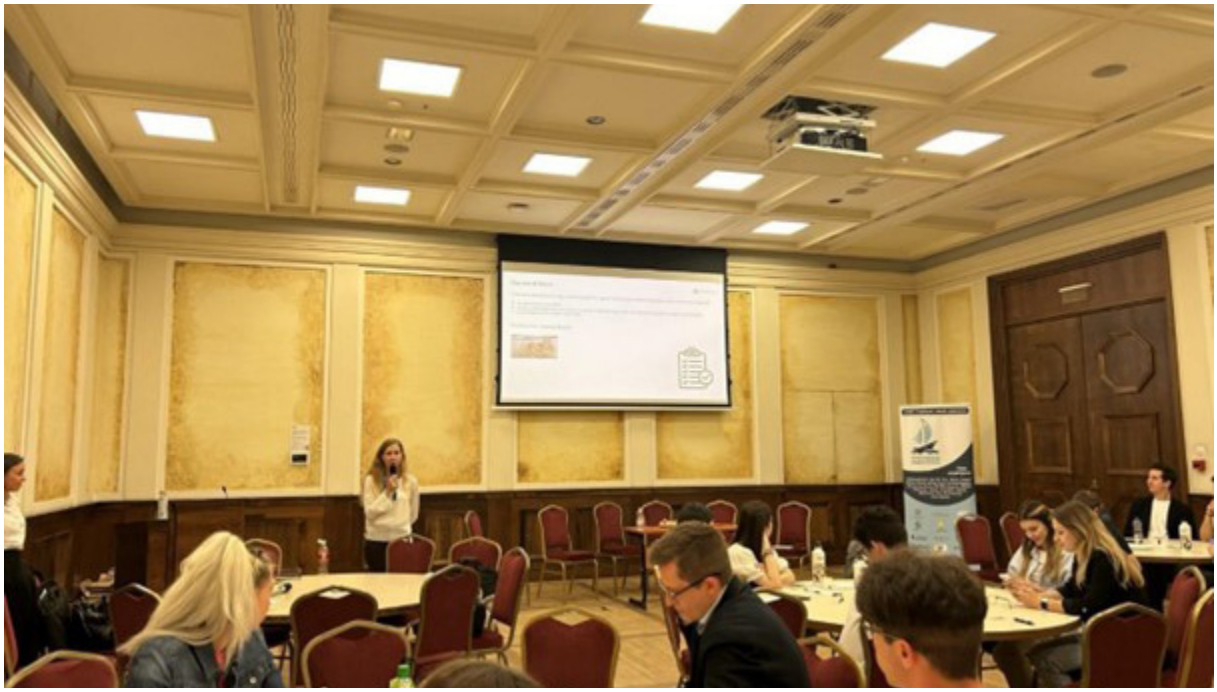
A Covid okozta kényszerdigitalizáció és az, hogy a vezetők egyre inkább a fiatalabb generációhoz tartoznak, azt eredményezték, hogy a magyarországi kkv szektor több lépést tett előre az adatalapú működés tekintetében, azonban még mindig bőven van hova fejlődni. Láthatóan a digitális pénzügyek a húzóágazat, ehhez lenne fontos felzárkóztatni a szervezeti adatok gyűjtését és alkalmazását, valamint az egyre fontosabbá váló informatikai biztonság területét. Az a cél, hogy a biztonsági jogszabályoknak való megfelelés ne csak egy kipipálandó megszorítás legyen, hanem ezek az intézkedések valóban a folyamatos, veszteségmentes működést biztosítsák. A tudatosítás rendkívül fontos, de sajnos nem csodafegyver, vezetői elköteleződés nélkül nem vezet eredményre. A hálózatosodás egyik legeredményesebb eleme a nagy port kavaró súlyos biztonsági incidensek tapasztalatainak és következményeinek megosztása. Azonban fontos, hogy a „ráijesztés” után legyen hova fordulni, a kkv-kat támogató szervezetek, egyetemek, kamarák ezzel tudnak a szektor fejlődéséhez hozzájárulni. Sérülékenység-vizsgálati, tanácsadói és fejlesztési szolgáltatások nyújtásával azok számára, akik felismerték – ahogy Kott Ferenc fogalmazott –: „Nem az a kérdés, hogy lesz-e valakinek IT-biztonsági incidense, hanem sajnos az, hogy mikor.”

Vállalkozásfejlesztés mesterszak szakmai nap

2024. május 24-én immár második alkalommal került sor a vállalkozásfejlesztés mesterszakos hallgatók egész napos szakmai és csapatépítő rendezvényére. A nap során sokféle élményben lehetett része a hallgatóknak: Balogh Péter startup előadásától a közös pizzázásig, a GE Vernova lean menedzsment workshopjától a vezetett borkóstolóig gazdag programmal készült a Vállalkozás és Innováció Intézet csapata.

A sűrű napot az AmCham és a Magyar Kockázati- és Magántőke Egyesület szervezésében megrendezett Start Your Business rendezvény nyitotta, amelyben sikeres vállalkozók és kockázati tőkebefektetők osztották meg tapasztalataikat a hallgatókkal. Balogh Péter (STRT alapítója, korábban NNG társalapító és nem mellesleg a Cápák között műsor cápája) a startupok rövid innovációs ciklusairól, Szalay Kristóf (a TURBINE AI társalapítója) a korai vállalkozói élményeiről, azok tanulságairól beszélt, amelyet egy panelbeszélgetés követett, ahol a diákok is feltehették kérdéseiket a vállalkozásalapítás és -finanszírozás témakörében.

Miután a mesterszak hallgatói ünnepélyes keretek között átvették az okleveleiket a tantermen kívüli extra teljesítményeikért, a Vállalkozásfejlesztés Alumni Mentorprogram néhány alumnusával is beszélgettünk a karriertervezés kihívásairól. A jól megérdemelt (az Ifjúsági Vállalkozáselénkítő Egyesület és a GE Vernova támogatásával az asztalokra került) pizzák elfogyasztását követően a szakhoz közvetlenül kötődő diákszervezet, a Vállalkozásfejlesztés Klub mutatkozott be és szervezett csapatépítő játékokat a hallgatóknak. A délutáni szakmai program a lean menedzsment praktikáira fókuszált, amelyeket a GE Vernova kollégái (Szigel Márta és Harcsás Dorina) rendkívül gyakorlatiasan és játékos feladatokkal illusztrálva mutattak be a hallgatóságnak.



A napot ezután egy borkóstoló zárta Dr. Fiáth Attila vezetésével, melyen a hallgatók egy barátságos verseny keretei között összemérhették és gyarapíthatták is a hazai borokkal kapcsolatos ismereteiket. A változatos programoknak köszönhetően a rendezvényen részt vevő közel 70 hallgató nemcsak jól szórakozott, hanem friss tudással és erős közösségi kötelékekkel is gazdagodott. Jövőre folytatjuk!