Az informatikai szakemberek erkölcsi felelőssége

Interjú dr. Göcs László egyetemi adjunktussal

DOI: 10.14267/VILPOL2024.05.15

Dr. Göcs Lászlóval, a Neumann János Egyetem oktatójával és elismert informatikai igazságügyi szakértővel beszélgettünk a kiberbiztonság aktuális kihívásairól, a technológiai fejlődés hatásairól, valamint a magyar vállalatok kiberbiztonsági tudatosságáról.

Új lehetőségek a kiberbűnözők számára a pandémia idején

A COVID-19 világjárvány hatására az emberek és vállalatok világszerte fokozottan tértek át a digitális megoldásokra, legyen szó munkavégzésről, online kereskedelemről vagy ügyintézésről. Ez a folyamat a digitális tér bővülését eredményezte, ami viszont magával hozta a kiberbiztonsági kockázatok drámai növekedését.

Göcs hangsúlyozta, hogy a kibertámadások és csalások száma az elmúlt években megsokszorozódott, gondoljunk csak a futárszolgálatok nevében elkövetett hamis SMS-ek eseteire. Ennek oka, hogy az online jelenlét bővülése, különösen a járvány idején, új lehetőségeket nyitott a bűnözők számára, hiszen egyre több lehetséges célponttal rendelkeznek.

Göcs László külön kitért arra is, hogy a kiberbiztonsági szabályozások globális szinten is egyre nagyobb figyelmet kapnak. A TikTok körüli szabályozások példája jól mutatja, hogy a technológiai vállalatok által gyűjtött adatok milyen mértékben jelentenek nemzetbiztonsági kockázatot.

A banki csalások Magyarországon is jelentős károkat okoznak, **2023-ban 24 milliárd forintot veszítettek el a banki ügyfelek csalások miatt.**

Ez a szám már nemzetgazdasági szinten is problémát jelent, hiszen az összegek külföldi számlákra vagy kriptovalutába kerülnek át. Az EU-ban a geopolitikai kockázatok miatt Göcs a központosított adatkezelés híve, ami szerinte kulcsfontosságú lenne a biztonság növelése érdekében. Hangsúlyozta, hogy a központosítás nemcsak technikai kérdés, hanem gazdasági és politikai szempontból is előnyös lehet, különösen a nagy volumenű adatkezelési rendszerek, mint például az Ügyfélkapu esetében. Ugyanakkor elismerte, hogy a központosítás nehézségekkel járhat, például a biztonságos jelszavak és a többfaktoros azonosítás terén, de hosszú távon ez a megközelítés javíthatná a digitális rendszerek biztonságát.

Az emberi sebezhetőségek: A kiberbiztonság gyenge láncszeme

Göcs László rámutatott, hogy az informatikai rendszerek gyorsasága és kényelme gyakran a biztonság rovására megy. Az emberek hajlamosak az egyszerűbb megoldásokat választani, például egyetlen jelszót használni több helyen, vagy a vezérigazgatók kerülik a kétlépcsős azonosítást időhiány miatt. Bár a technológia gyorsan fejlődik, ugyanez igaz a támadási módszerekre is, különösen a mesterséges intelligencia (MI) terén. Az MI képes gyorsan átfésülni adatbázisokat, és alapot nyújt az automatizált támadásokhoz, így növelve a kiberbiztonsági kockázatokat.

A kiberbiztonsági tudatosság növelésében lehet a megoldás

A kiberbiztonság megteremtése terén a Neumann János Egyetem fontos szerepet vállal, különösen a prevenció területén. Az egyetem Kecskeméten együttműködési megállapodást kötött a Bács-Kiskun Vármegyei Rendőr-főkapitánysággal, akikkel közösen dolgoznak ki oktatóanyagokat, majd ezeket eljuttatják általános- és középiskolákba, idősek klubjaiba és az iparkamarán keresztül a vállalatokhoz.

A cél, hogy a társadalom széles körében érthetően és érdekesen mutassák be a kiberbiztonsági veszélyeket, valamint azokat a módszereket, amelyekkel ezek a támadások megelőzhetők. Az egyetem és a rendőrség közös munkájának köszönhetően a kiberbiztonság tudatossága növekedhet, különösen a fiatalok és az idősek körében, akik gyakran válnak a digitális bűnözők célpontjává.

Göcs László szerint nehéz meghúzni a határt a vállalati és a személyes felelősség között a kiberbiztonságban, különösen, ha az emberi tényező szerepet játszik. Míg a felhasználót gyakran hibáztatják, a megtévesztés esetén a felelősség kérdése bonyolultabb. Göcs kiemelte, hogy a felhasználóknak el kell különíteniük a magánéleti és a vállalati tevékenységeiket.

„Például, ha egy céges laptopot otthon használnak, nem szabad hagyni, hogy a gyerekek azon játszanak, miközben a gép akár a vállalati hálózatra csatlakozik, mert ez súlyos biztonsági kockázatot jelenthet.”

Alkalmazkodás a NIS2-hez: A magyar cégek előtt álló út

A magyar vállalatok kiberbiztonsági tudatossága sajnálatos módon alacsony szinten áll. Göcs László szerint ez nem ágazati és nem pénzügyi kérdés, a választ a humán erőforrásokban kell keresni: a tudatosság és a vezetői felelősség hiányának következménye. A NIS2 irányelv bevezetése, amely az EU-ban a hálózati és információs rendszerek biztonságát szabályozza, hasonló hatást gyakorol majd a vállalatokra, mint korábban a GDPR.

Úgy véli, hogy az EU-s adatvédelmi szabályozások nagyon fontosak a hazai vállalatok számára is, de nagyon sok esetben még az alapszintű kibervédelem sincs megvalósítva. Egyes vállalatok olyan egyszerű problémákkal küzdenek, mint a nem biztonságos wifi használat vagy a felhasználói jogosultságkezelés hiánya, először ezeket az alapvető területeket kellene megoldani.

Számos esetben először az ISO 27001 standardot kellene elérni, mint a NIS2-t. Ettől függetlenül elmondható, hogy a GDPR pozitív hatást gyakorolt az adattárolásra, mivel sok vállalat titkosítási technológiákat vezetett be a szervereken, de a kiberbiztonsági kockázatok csökkentése érdekében még sok tennivaló van.

Az irányelvnek való megfeleléshez szükséges auditálás is komoly kihívást jelent, mivel a kritériumok hosszú listája miatt sok vállalatnak jelentős átalakításokra lesz szüksége. A jelentős mennyiségű anyag feldolgozásával jellemzően a fiatalabb informatikus kollégákat bízzák meg a vállalatokban, más esetben a növekvő népszerűségnek örvendő NIS2 tanácsadókra bízzák ezen feladatokat. Göcs emellett arra is rámutatott, hogy a meglévő erőforrásaikat sem használják ki a vállalatok megfelelően: előfordul, hogy olyan drága hálózateszközeik vannak, amelyek képesek komoly biztonsági paraméterekre, de ezek nincsenek alkalmazva.

A jövő kiberbiztonsági munkaereje

Egyre inkább elmondható, hogy az informatikai vezetők feladatkörébe nem pusztán technikai problémák esnek, hanem feladatuk az is, hogy felismerjék és érthetően kommunikálják a kiberbiztonsági kihívásokat az üzleti vezetők felé, akik nem a technikai részletekben szeretnének elmerülni. Tehát a megfelelő kommunikáció kulcsfontosságú, és a Neumann János Egyetemen is hangsúlyt fektetnek a hallgatók ilyen irányú fejlesztésére.

Az egyetemen például többek között szóbeli vizsgákat is tartanak, hogy a jövő informatikusai megtanulják, hogyan kommunikálhatják hatékonyan az ajánlásaikat a vezetők felé. Emellett kiberbiztonsági és hálózatbiztonsági tárgyakat is oktatnak, amelyek nélkülözhetetlenek lesznek a jövő munkaerőpiacán.

Göcs az informatikai szakembereket az orvosokhoz hasonlítja, mivel mindkét szakmában szerteágazó szakterületek vannak. Azonban a kibervédelmi szakértőknek, hasonlóan a háziorvosokhoz, átfogó ismeretekkel kell rendelkezniük, beleértve a hálózatokat, adatbázisokat, fejlesztést, dokumentációt és jogszabályokat. Az egyetemi diploma csak belépő a szakmába; a piacon számos szakmai tanúsítványt is szükséges megszerezni a könnyebb elhelyezkedés érdekében, amiben az egyetem is igyekszik támogatást nyújtani.

Az etikus hacker terület kiemelten nagy népszerűségnek örvend a hallgatók körében, azonban az interjúban az is kiderült, hogy milyen alapvető problémával lehet találkozni ezen a pályán. Aki csak úgy etikus hackernek képzeli magát, és talál sérülékenységet egy rendszerben, az kellemetlen helyzetbe hozhatja az adott cég IT vezetőjét. A cégvezető ugyanis a sérülékenység felderítése után az IT vezetőt hibáztathatja a rendszer gyengeségei miatt, ami feszültséget szülhet. Ilyen esetekben a magát etikus hackernek mondó nem dicséretet kap, hanem a megtámadott fél akár a Nemzeti Nyomozóirodához fordulhat a helyzet tisztázása érdekében. Csak az az etikus hacker, akit hivatalosan, szerződéssel megbíznak a sérülékenység felderítésére.

Göcs megvilágította, hogy az informatikai szakemberek erkölcsi felelőssége különösen nagy, hiszen ők férnek hozzá a vállalatok legérzékenyebb adataihoz. Az emberi érzések, mint a boszszú is kockázatos lehet: ha egy IT-szakembert elbocsátanak, de a vállalat pl. nem gondoskodik megfelelően a jogosultságkezelésről, mesterkulcsok elzárásáról, az elbocsátott alkalmazott hatalmas károkat okozhat a cégnek.

Szabó Csege