***Vágner Máté*[*]:**

AZ IOT BIZTONSÁGVÉDELMI KIHÍVÁSAI ÉS A KIBERTUDATOS FELHASZNÁLÓVÁ NEVELÉS

A projektem témájának középpontjában az IoT-s (Internet of Things - A Dolgok Internete) eszközökkel kapcsolatos és az általános kibertudatosság, és annak növelési technikái állnak. Ezen kívül megvizsgáltam a kibertudatosság hatásait a hétköznapokra, a biztonságra, az üzleti életre, a kultúrára és a bűnözésre is.

Kutatásomat az inspirálta, hogy tömeges figyelmetlenséget láttam a területtel kapcsolatban. Például részt vettem egy háromhónapos startupképzésen, ahol egy táplálékkiegészítő turmixot készítő csapat nem is gondolt arra a lehetőségre, hogy komolyabban titkosítsák a felhasználó bankkártyaadatait az eszköz és a router között, így bárki ellophatta volna ezen adatokat 100 méteres körzeten belül. Hasonlóan ijesztő példa a Deutsch Telecom felmérése, ami alapján ügyfeleik csupán 12% fordít megfelelő figyelmet az okoseszközei védelmére. Ezeken kívül más elrettentő példákkal is találkoztam, mire kutatásom megírtam.

Az IoT

A téma megértéséhez előbb szükséges az IoT és működési alapjainak ismerete. Általában azon eszközöket soroljuk a csoportba, amelyek más eszközzel vagy eszközökkel kétirányú kommunikációt folytathatnak. A működés közben keletkező adatokat, információkat képesek más berendezésekre eljuttatni, és valamilyen technológia segítségével, akár netes adatbázisok, felhőalapú rendszerek révén a világ bármely pontján megosztani, ezzel segítve a gépek intelligens döntések meghozatalában.

Az IoT megállíthatatlanul fejlődik. 2016-ban 6,4 milliárd IoT eszköz volt használatban, ami a Cisco becslései szerint 50 Milliárdra nő 2020-ra. Húzóágazatnak számít az Ipar 4.0 (azaz a személyre szabott termékek gyártásának lehetősége) – például a Harley Davidson IoT gyártógépsorán az egyedi motorkerékpárok már 2 hét alatt elkészülnek az eddigi 18 hónap helyett – és az okosházak (1. ábra) is. Az okosotthonpiact 20020-ra 60 milliárd $-osra becsülik. [1]

Az IoT lényegében a számítógépek újtípusú perifériái. A hagyományos egér/billentyűzet párost egészíti ki és majd talán le is váltja egyszer. Lényegében ezen eszközökkel lehetővé tesszük a gépek számára az érzékelés lehetőségét is a többi eszköz adatai alapján, hogy együttesen intelligensebb döntések hozhassanak. Például a közlekedés biztonságosabbá tételének céljából fejlesztett okosautókban található szenzorok és adataik felhőben történő feldolgozása is ezt a feladatot tölti be.

Az IoT növekedési üteme is kiemelkedő. Az ezközök száma 5x gyorsabban növekszik, mint ahogy az elektromos vagy rádiókommunikációs eszközök terjedtek. Az ezközök már most napi 5TB adatot állítanak elő és töltelen fel a felhőbe. Tehát az IoT már most egyértelműen az informatikai fejlődés következő lépésének lehet nevezni.

A rendszer terjedése még tovább gyorsulhat az 5G technológiának köszönhetően, ami lehetővé teszi, hogy egy hálózati elosztóközpont egyidejűleg több millió okoseszközt szolgáljon ki, mindezt az eddigiekhez képest fajlagosan alacsonyabb energiafelhasználással.

A problémák

Hardveres és szoftveres oldal

Hatalmas problémát jelent elsősorban a gigabotnetek jelenléte. Ezek olyan „zombi” eszközökből álló hálózatok, amik parancsra bármelyik nagy hálózatot vagy weboldal ellen DDoS (Distributed Denial of Service - elosztott szolgáltatásmegtagadással járó támadás, ami alatt rengeteg gép terhel túl egy szervert egyidejű adatlekéréssel [2]) támadást hajthat végre a vírus által megfertőzött eszközökkel. A

[*] Köszönet Kasza Tamás, Szilágyi László, Jakab Roland és Vágner Richárd Attila Mentoraim támogatását és önzetlen együttműködését. Köszönet továbbá mindenkinek, aki részt vett a közvéleménykutatásaimban és felméréseimben.

második legnagyobb eszközszámmal rendelkező ilyen hálózat a Mirai. Ennek a veszélye az, hogy a 223000 megfertőzött eszközzel – a vírus nyílt forráskódjának köszönhetően – bárki támadást hajthat végre bármilyen szerver ellen. A legnagyobb a Bashlight zombihálózat közel 1 millió fertőzött eszközzel [3].

Ezen vírusok támadásaival közkedvelt oldalakat lehetetlenítenek el a működétől rövidebb vagy hosszabb ideig. Ezen hálózatok továbbá megkönnyítik a kiberbűnözők tevékenységét és elbújását, mivel a felderítésüket a rengeteg átirányítási lehetetlenné teszi.

Ezen támadások elhárítására és megelőzésére pont az előbbi veszélyek miatt a szakma sok figyelmet szentel. Megpróbálják szoftvereik, hardvereik biztonságossá tenni. A cégek egyre jobban elkezdenek odafigyelni a veszélyekre és államunk felelős szervei is egyre komolyabb munkát végez a helyzet javítására. A megfertőződéseknek pont emiatt egyre inkább a hétköznapi emberek által használt akár titkosítás nélkül hagyott vagy elfelejtett, a periférián maradó IoT-s okoseszközök vannak kitéve. Emiatt is lett kutatásom fő irányvonala a hétköznapi felhasználók oktatása.

A leggyengébb láncszem – az emberi tényező

A felhasználó tudatosság az előző pontban leírtak miatt egy nagyon fontos tényező a jelen és a jövő kibervédelemben. Mert hiába fáradoznak a IT biztonsági szakemberek, hiába győzik meg a programozókat biztonsági protokollok használatáról, ha a felhasználók nem figyelnek a biztonságra a használat során.

A felmérések alapján hazánknak is, de a világon szinte mindenhol bőven van még hova fejlődni a kibertudatosságban. [4] A hétköznapi felhasználók nagy része, sőt a munkaadók közül a nagyvállaltok fele, míg a közép- és kisvállalkozások csupán 10%-a figyel oda rá. A legutóbbi, csak közalkalmazottak által kitöltött kutatás alapján szükséges az IT tudatosság fejlesztése és mérése is, mivel ezen területre csak 70%-ban érkeztek helyes válaszok. Egy kutatás alapján [5] a felhasználók 25% nem is akar foglalkozni az ilyen típusú biztonságvédelemmel, 56% nincs tisztában a honlapok megtekintésének biztonsági szabályaival, 40% beismeri, hogy nem venné észre, ha feltörnék eszközét, mégis ezen felhasználók fele elégedett informatikai tudásával. Továbbá a megkérdezett felhasználók 84% nem bízik a vírusírtókban, tűzfalakban, mégis 60% azt állítja, hogy ő felismerne egy vírust. Ezen adatokból jól látszik, hogy a képzettebb felhasználók között is hiányosságok vannak, és a nem megfelelő tudás, valamint a hamis biztonságérzet is egy komoly problémát jelent.

A projektben én is végeztem egy kutatást. Erre csak 28-an válaszoltak, de egy széles társadalmi körből. Ez alapján látszik, hogy az emberek nem érzik maguk otthon az IoT területén, de még nem is használnak sok okoseszközt. Viszont elképzelhetőnek tartják, hogy több ilyen eszközt is beszerezzenek a jövőben. Számukra a legfontosabb az eszköz ára, hasznossága és érdekli őket az egyszerű kezelhetőség, egy független szervezett tesztje, ismerősük ajánlása, valamint a gyártó megbízhatósága is. Ennek ellenére nem venné figyelembe az általa választott hálózati kommunikációs platform sebezhetőségét, és 56% nem tudja, hogy támadás esetén kihez forduljon.

Az otthoni hálózatforgalomfigyelő eszközökről is csak 21% halott már, viszont a képességei megismerése után 70% szerint hasznos lehet, 40% venne is, ha hazánkban is is árusítanának ilyeneket, valamint tudástól függően átlagosan 5-30 ezer forintot fizetne érte, de akár 60 ezer forint feletti összeget is képes volna fizetni érte, ami piacot adhatna hazánkban is ezen eszközöknek.

Az ember a gép mögött

Ennek a problématerületnek a kezelése adhatja a kiberbiztonsági büdzsé legnagyobb részét, de, ahogy láthattuk, a IT biztonságtudatosság nélkül a szakemberek erőlködése alig ér többet egy fabatkánál. Fontos kiemelni, hogy *az emberi tényezőhöz teljesen máshogy kell hozzáállni, mint az alapszintű gépi biztonsághoz!*

A problémák sikeres megoldásához és megértéséhez először meg kell lelni az embert a gép mögött. Az ember a géphez viszonyítva máshogy gondolkodik (Például tökéletlen, de ezt nem szereti beismerni, míg egy géppel könnyebb dolgunk van, aki csak azt csinálja, amit mi mondunk neki.), gondolati sémáit nem lehet a gépekéhez hasonlítani. Emiatt szükséges a türelmes kommunikáció és a személyiség figyelembevétele is. Az oktatási, a felnőttképzési és a pszichológiai szakembereket is

be kell vonni a probléma kezelésébe. A szükséges intézkedésekhez együttműködés is szükséges a cégek és az állam között, ami ugyebár az üzleti versenyhelyzet miatt nehézséges lehet, de meg lehet győzni a feleket a minimális együttműködésről, ami már hatalmas segítséget lehet.

Ezentúl ebben egy hatalmas értékteremtő lehetőség van, ugyanis a megfelelő figyelem és társadalmi elemzés segíthet az ember jobbani leírására az informatika nyelvén, ezzel hozzájárulhat a gépi gondolkodás és tanulás területén végzett kutatások sikeréhez is. Így lehetőség nyílik a programozóknak és az informatikai szakembereknek jobban megismerni az emberi gondolkodásmódot és döntési mechanizmust. És az ilyen típusú koordinált kutatások több tőkét hozhatnak be a rendszerbe.

A kezelési lehetőségek

Üzlet és biztonság

A szakértők szerint pont a fentiek miatt kiemelt figyelmet kell szentelni ezen eszközöknek a sikerért. [1] Érdemes összefogni a fejlesztésük területén, oda kell figyelni a tudományos fejlődés és a termelékenység egyensúlyára.

Az informatikán belül jelenleg ebben van a leghatalmasabb fejlődési lehetőség, de cserébe ez tartogatja a legtöbb kibervédelmi és biztonsági rést, amik az idő múlásával egyre gyorsabban fognak felbukkanni. Emiatt tényként kell kezelni a jövőben a területet érintő hackertámadásokat, és fel kell készülni rájuk. Úgynevezett „reagálási tervet” kell készíteni a cégeknek és az országoknak különböző támadásokra. Ennek tartalmaznia kell a támadások megelőzését, a támadások mihamarabbi észrevételét, a rendszerek fölötti uralom visszavételét és a helyreállítást is. Az IoT-t emiatt sose szabad egyszeri beruházásként kezelni. Folytonos frissítést, karbantartást és felügyeletet igényel.

Az emberek féltik személyes adataikat, csak sokukban mégsem tudatosul az, hogy figyelmetlenségükkel ezek biztonságát veszélyeztetik. Az emberek igénylik a biztonságot, erre képesek akár pénzt is áldozni, és minimális szinten lemondani egyes adataik saját megvédéséről, ezt a feladatot bizonyos adatok alapján cégek számára kirendelni.

A felhasználók egy része mindenáron az adatai privátság akarja megőrizni, míg egy másik komoly csoport adatai biztonságát félti, és ezért képes ezt második féllel is megosztani, ha harmadik fél nem juthat hozzá. Viszont nagyon nem értékelik, ha harmadik fél is megkapja az adatokat. Ezt bizonyítja például a Facebook adatbotrány is. [6]

Az okoseszközpiacon is az lesz a jövőben versenyképes, aki viszonylag hamar, stabilan tudja biztosítani ügyfelei és vásárlói biztonságát. Biztonsági cégek számára fontos lehet ezért a rendszeres önátvilágítása. A titkosítást végzők és a biztonságért felelősök jó, ha a kezelt adatok miatt nyíltan megbízhatók.

A felhívás fontossága

A vállalatok számára fontosak a folytonos cégen belüli és kívüli elemzések, mivel az ügyfélkör és a munkavállalók tudatossága is fontos, főleg az ipar 4.0 alapú gyárak esetében, mivel itt a kész termék legtöbb esetben kapcsolatba léptethető a gyár rendszerével, és így egy végfelhasználónál történt szivárgás az egész vállalatot is érinti.

Ugyanakkor az állam számára is fontos az emberek tájékoztatása, mivel az eszközök mindenki saját maga általi felügyelete elősegítené a kiberbűnözők megfékezését. Ha nem tudnának hálózati átjátszásokon keresztül elbújni, akkor sokkal nehezebb dolguk lenne.

Tehát a rendszer gyengeségeinek kiszűrése, megértése és rendszerszintű, akár technológiával, akár továbbképzéssel és a kiberérzékenység finomításával, kiépítésével történő erősítése szükséges. Fontos továbbá az ezek közötti egyensúly megtalálása is. Itt fontos feladatköre van az összes felelős szervnek, valamint közösségnek is.

Ezzel egy tárgyalóasztalhoz lehet ültetni mind a felelős szerveket és mind a cégeket is, mivel mindnyájuk profitálhat belőle, és a minimális együtt működés nem feltétlen járna vállalati titkok feltárásával (amik a cégek legféltettebben őrzött kincsei), hanem az emberek képzésének, tájékoztatásának koordinációja lenne, ami így csökkentené az ehhez tartozó pénzügyi terheket a partnerekre nézve.

Hasonló célú kezdeményezések szerencsére már hazánkban is létrejöttek, amik támogatandók. Ilyen például az Ipar 4.0 Nemzeti Technológiai Platform Szövetség [7] is. Ezen szerveződések viszont felvehetnék a mélyebb felhasználói tájékoztatást is a tevékenységeik közé, a fent említett okok miatt.

A felhasználók felkészítése

Mindezek mellett az embereket is fel kell készíteni a sikeres megelőzésre és a támadásokra való reagálásra. Mivel az IoT lesz a legnagyobb perifériafelület és kommunikációs platform, emiatt a jövő emberének naprakésznek kell lennie és a megfelelő tudás birtokában kell használnia az eszközeit.

Elsősorban az embereket tájékoztatni kell az okoseszközök megfelelő felhasználásáról és helyükről a mindennapi életben. Tehát a szakmán belülieknek egyértelműnek tűnő, de a marketinggel bombázott hétköznapi embernek nem egyértelmű dolgokat is tudatosítani kell az emberekben. Ilyen például az átlagos marketingfogás, hogy az okoseszközök összehangolt működése energiát spórolhat meg nekünk. Ez igaz, de csak abban az esetben, ha már alapból viszonylag sok okoseszközt használunk. Mivel, ha csak most szerelünk be okoseszközöket a házába, akkor lehet, hogy ezek az eszközök kezeléséért felelős okos és energiatakarékos energiafogyasztás mérő eszközünk majd arról informál minket, hogy drasztikusan nőtt a fogyasztásunk, mivel az újonnan beszerelt új kiegészítők mind több árammal működnek, mivel a több képesség, több számítást, a több számítás pedig nagyobb áramfogyasztást jelent. Továbbá szükséges a megfelelő infrastruktúra meglétét is hangsúlyozni az összes beruházás előtt, mert a nem megfelelő körülmények nagyobb kárt tehetnek az eszközökben, mint amennyi hasznot azok hozhatnak.

Nem mind arany, ami…

Továbbá meg kell hallgatni az IoT-vel kapcsolatos kritikákat. Egyik ilyen az IoT „Bénaságok internete” gúnyos elnevezése, ami arra utal, hogy mostanában külföldön rengeteg, a civil vagy egyéb informatikán kívülről jövő startup kezdeményezések voltak, amik során sokszor teljesen hasztalan, vagy át nem gondolt, a biztonság legkisebb gondolatát is nélkülöző eszközöket fejlesztettek. A felhasználókban tehát tudatosítani kell, hogy nekik is keresni kell a ténylegesen értékes és okos IoT eszközöket, mivel egy eszköz attól, hogy össze van kapcsolva az internettel, még nem lesz okos.

Ebből adódóan szükséges a fejlesztési és vásárlási szokások együttes változtatása is. A két szférát közelebb kell tolni egymáshoz, mint ahogy a nagyobb cégek ezt már meglépték. Fel kell hívni a figyelmet a tudatos vásárlásra és tudatos fejlesztésre!

A fejlesztőknek az eszközük biztonságra, fentarthatóságra kell törekedniük. Természetesen ismerniük kell a felhasználási területeket, a felhasználókat, tudásukat, gondolkozásmódjukat és azt, hogy mi fontos számukra. De mindezek mellett nekik is tisztában kell lenniük az informatika alapjaival, a biztonság fontosságával és a felhasználók látásmódját az informatikusok felé is képviselniük kell, hogy az eszközt fejlesztő informatikusok is a felhasználó szemszögéből is könnyű használhatóságra törekedjenek.

A felhasználóknak pedig mérlegelnie kell ezek alapján, hogy neki mire van szüksége. Ehhez segítséget nyújtó alapszintű kérdések találhatóak a kutatás III. Mellékletének 1. táblázatában.

A tájékoztatás

Elsősorban trenddé kell tenni a „kiberérzékenységet”. A kutatásom alatt azt láttam, hogy az emberek alapjáratban szeretnek trendeket követni, és ebből mi magyarok sem maradunk ki. Viszont a népünkbe van egy erősebb tartás a külföldről jövő befolyásoló erőkkel szemben (valószínűleg ezért is maradhattunk meg magyarnak már több mint egy évezreden keresztül). Társadalmunknak fontos, hogy belülről jövő kezdeményezések mögé tudjanak beállni. Így lehet lehetőségünk Magyarországon divattá tenni az információbiztonságra való érzéket.

Viszont nem csak a figyelmet kell felhívni. Az elrettentő történetekkel nagy hírt lehet kelteni, de ez mit sem ér, ha nem adjuk meg az embereknek a döntésekhez szükséges tudást és nem adunk nekik tanácsokat. Ilyen tippekből álló táblázatokat tartalmaz a kutatás III. Mellékletének 2. és 3. táblázatában [8][9]. Ezekhez hasonló, szemléletesebb, ámde ezen információkat mindenképpen tartalmazó tanácsadási listát kell összeállítani, ami alapja lehet az IoT biztonságvédelemnek és a

hackertámadások megakadályozásának. Egy ilyet és tippjeit mindenképpen minél több embernek át kell átadni.

A sikeres felszólításhoz szükséges a felhasználók ingerküszöbének megugrása is, ami nem mindig egyszerű feladat. Ehhez jó eszközök lehetnek a szokványostól eltérő ismertető ábrák (pl. kézi rajzok) vagy fontos személyek harcba állításával a téma mellett. Kiberkárjelentésekkel, bemutató műsorok készítésével és annak a ténynek az ismertetésével, hogy mennyire könnyen feltörhetőek az eszközök a megfelelő védelem hiányában. A felhasználók nagy része felfigyel, ha ismertetik vele sebezhetőségét.

Felnőttképzés a jelenért

Nagy figyelmet kell fordítani a szükséges információk átadására már a tapasztaltabb generációk számára. Ebben fontos szerepe lehetne a felnőttképzésnek és a munkaadók által szervezett továbbképzéseknek is. Létre lehetne hozni egy ECDL-hez hasonló vizsgarendszert, ami keretében a munkavállalók biztosíthatnák, hogy rendelkeznek azzal a tudással, amivel felelőségteljesen és biztonságosan tudnak felhasználói lenni a kibertérnek és informatikai eszközeiknek.

A végfelhasználók meggyőzhetők, mivel nagy eséllyel áldozatai, de szinte mindig negatív érintettjei a támadásoknak. Vegyük például a 2017-es kibervihart, ami alatt több nagycég között a Facebook is átélte eddigi talán legnagyobb DDoS támadását. Ebben az esetben nemcsak a Facebook esett el nagy bevételektől, de egy hosszú ideig a felhasználók se használhatták az oldalt, tehát az általuk nem megvédett zombieszközök támadása őket is negatívan érintette.

Meg kell teremteni a kibervédelem kultúráját! Ebben segíthet, hogy ha a felhasználókban elvárásokat támasztunk magukkal szemben és jó viselkedésképet alakítunk ki bennük jó példák mutatásával. Az információbiztonságra való érzékenységet akár a kultúrtermékekbe (filmek stb.…) is be lehet építeni a társadalom nevelése céljából.

Nem felejthető el az se, hogy az emberek oktatása nem egyszeri feladat. A tudást minimum évenként meg kell újítani. Tájékoztatni kell mindenkit az aktuális veszélyekről és védekezési lehetőségekről. A képzések sikerét és hatékonyságát növelheti, ha személyessé, interaktívvá tesszük őket, hogy saját ügyüknek érezzék ezt a munkát a felhasználók. A képzések folyamatát pedig felügyelni kell! Ellenőrizni kell a hatékonyságát, a résztvevők elégedettségét. Ha valahol baj van, akkor módosítani kell rajta. A fő pontokat is rugalmasan kell kezelni, mert előfordulhat, hogy az érzékenységi területek változhatnak az idő múlásával. Lehet, hogy egyszer a biztonság, másszor a privátság vagy a nettől való függetlenség lesz az embereket legjobban megfogó téma. Az átadandó információkon és a képzéseken is valószínűleg mindig lehet majd változtatni valamit, tehát soha se szabad megkötni a tananyagot, hanem engedni kell folytonos kialakulását

Továbbá segít, ha sikerül mindennapi témává tenni a kiberbiztonságot. Ez elérhető például társadalmi viták, konzultációk kezdeményezésével vagy rendszeres munkahelyi hírlevelekkel, amik még az emberek informáltságát még naprakészebben tartja.

Közoktatás és egyetemi képzés a jövőért

A fent leírt képzések hasonlóan alkalmazhatóak itt is. Akár a tananyag részeként, akár különálló képzésként is, csak a gyermekek képességeihez és érdeklődési köreihez igazítva. Itt fontos a gyerekekben korán kialakítani a kiberérzékenységet és kiemelni a gondolatmenet fontosságát. Tanulják meg, hogy egy támadó fejével is kell tudni gondolkodni. Ez a képesség nagyban hozzájárul a jövőbeli sikeres megelőzéshez és a megfelelő válaszadáshoz is.

A középiskolai osztályfőnöki órák, szakkörök és akár kutatások témái közé is be lehetne emelni a témát. Sőt, akár a hivatalos szervek is rendezhetnének kiszállásos előadásokat, vagy akár a témához köthető versenyeket a diákoknak.

Az is segítene, ha minimális szinten, de indulnának kibervédelemre szakosodott képzések vagy szakok is. Továbbá egyes kibertámadások forgatókönyveit és reagálási terveit egyetemi labormunkaként, kutatásként, valamint diplomamunkaként történő megvalósítását is támogatni lehetne.

Továbbá megpróbálhatjuk kiszűrni a jövőbeli hackereket az iskolarendszerben. A tehetségeseket felismerve még időben etikus, úgynevezett fehérkalapos hackereknek lehetne nevelni őket.

Az állam szerepe

Az eddig említett szerepek és hasznok az államot is érintették, de mégis mi lehet még a haszna és milyen feladatai lehetnek?

A fő kérdés az, hogy az adott nemzetközi helyzetben hol a határ? Mikor és meddig mehet el az állam a biztonság érdekében a személyi jogok kárára? Ezen kérdéseket lehetőleg előre tisztázni kell, mert más helyzetekben más fontos sz állampolgárok és az állam számára.

Kezdeményezhet az állam és a magánszektor közötti kiberproblémai információmegosztást. Ezzel tudhatjuk, hogy mi mindig a következő lépés a kibervédelemben, mire kell készülni. Ilyen kezdeményezés már van az USA-ban, de még lehet javítani rajta, mivel jelenleg csak kis hatásfokkal működik, mert a cégek félnek az online információtovábbítástól az internetes „adatlehallgató" vírusok miatt. [10]

Továbbá fel kell készülnie a kiberviharokra, miben a felsőoktatási laborok segítségre lehetnek.

Egy megemlítendő amerikai kezdeményezés a StaySafeOnline, ami nemzeti kibervédelmi szövetség kezdeményezése. Egy hasonló szövetséggel hazánkban is nagyobb figyelem érhető el a téma számára. Ugyanakkor egy másik meghonosítható tevékenység a témával kapcsolatos ismertetőanyagok készítése, amivel elérhető az állampolgárok éves szintű tájékoztatása a témáról. Ezeken keresztül lehetne átadni például a fentebb felsorolt tippeket az állampolgároknak.

Továbbá az államnak egy szervezettel biztosítani is tudja, hogy a valójában biztonságos eszközök ne kerüljenek köztörvényes bűnözők és feketekalapos hackerekhez. [11]

Nagyon jó jelnek számít a már elkezdet kibervédelmi stratégia fejlesztése, valamint az, hogy a jövő hadviselési frontjának tekintjük a kiberteret. Továbbá támogatandók a probléma nemzetközi, V4-es szintű együttműködéseken keresztüli megoldása is.

Újtípusú gazdasági modell

Az IoT biztonságvédelem viszont a piaci gondolkodásmód változását és üzleti modellváltását is igényli. Mivel jelenleg az okoseszközök üzleti modellje az Apple modellhez és a telefongyártók modelljeihez hasonlók. A készülékek árába beleszámolják a szoftverkarbantartási díjakat is. Ez a fajta modell azért működőképes mert az emberek a mobiljaik általában 2 évente cserélik. Ez a helyzet ugyebár közel se áll fent egy kazán vagy okos szenzoros egységek esetében, amiknél a minél hosszabb üzemképeség a fő szempont. Emiatt szükségessé válhat a rendszer védelmét és szoftveres támogatását külön kezelni a hardvertől, még jobban ki kell tolni a támogatási időszakot. Mivel ugyebár az emberek nem akarnak majd 2 évente okoskazánt cserélni, amikor a „buta" kazánokat szinte sose kell cserélni.

Megjelent egy modernkori jelenség, a szoftveres elavulás. Ez az eszközök szoftveres biztonsági rendszerének elgyengülését jelenti, amellett, hogy a hardver még bőven használható, csak veszélyessé válik annak használata. Ez tehát mutatja, hogy a feltűnő biztonsági résekre állandóan ki kell majd adni egy frissítést, és ennek költségeit fedezni kell lesz valahonnan. Erre megoldást jelenthet egy olyan szolgáltatásokat indítani a vállalatoknak, aminek szükséges része a biztonsági fejlesztés, így az ott alkalmazottak költséghatékonyabban ültethetők át a már eladott termékek szoftvereibe azonos kódolási nyelv alkalmazása esetén.

Miért nem zártad el az internetet? Avagy gazdasági kibervédelem

Nemrég ütötte fel a fejét a hír, hogy Amerikában az állam kitiltotta a többek között a Huawei termékeit a közbeszerzési pályázatokról, mivel a P10-es modell folytonosan továbbítja a szenzorjaival (például mikrofon) vett adatokat egy kínai szerverre, amihez nem világos, hogy ki is fér hozzá és ki nem, így szinte bármilyen adat ezek közül bárhova kiszivároghatott.

Hasonló eset történt egy másik amerikai céggel is, akinek az ipar 4.0-val gyűlt meg a baja. Nekik a vevőiknél történt adatszivárgás. Az adatok nem voltak megfelelően titkosítva azoknál, akiknek szállítottak, így az amúgy titkos árlistájukat megtudta egy másik beszállító, így állandóan képesek voltak alul licitálni őket, ellehetetlenítve ezzel a cég megrendelésekhez való hozzájutását. És nem csak egy ilyen eset volt, hanem több cég is feljelentést tett hasonló ügyben.

Az ilyen ügyek kezelését is segíthetik az eddig felsorolt eszközök és módszerek, de plusz dolgokat is el kell mondani. Az emberekben tudatosítani kell azt is, hogy az sem mindegy, hogy honnan és mit vesznek. Nem mindegy, hogy ki validálja az eszközöt! Mert lehet, hogy valamelyik ázsiai országból olcsón megvehető egy okoseszköz, de amennyiben ez adatszivárgást okoz, akkor már meg sem éri.

Vegyük például a most Amerikában berobbanó hangvezérelt eszközöket. Ha ezek még jobban elterjednek, és kicsiny hazánkban is elérhetővé válnak, már egyből nem lesz olyan vicces az, ha valaki akár a világ másik végén, akár a szomszédban tudja vezérelni a házamat az én saját hangmintáim alapján. Az okoseszközök csak addig segítenek nekünk, amíg mi irányítjuk őket.

Persze szükséges a második példa esetében tisztázni a jogban ilyenkor az összes résztvevő felelőségét és számonkérhetőségét is.

A probléma egységes kezelése azért fontos, mert nem egyből fejti ki a hatását, hanem folyamatosan. És mire már észrevesszük addigra már késő. Emiatt a területet kezelését nem lehet halogatni, főleg mert akár a nemzeti szuverenitást is veszélyeztetheti, mivel a kiszivárgott adatok akár külföldi államok kezébe is kerülhetnek. Ez az egyik gyanúja az USA-nak a Huawei esetében is, de ha nem is ez igazolódik be, akkor is hatalmas kockázatot tartogat a terület figyelmen kívül hagyása, mivel közel se mindegy, hogy ki validálja az eszközöket. Teljesen egészséges, ha az állam fenntartja az ellenőrzési jogát mind a kül- és belföldi beszállítókkal kapcsolatban is.

Egy kiberbiztonsági szervezet gazdasági fentarthatósága

Az eddigi összes pont tehát azt igazolta, hogy szükség van a kiberérzékenység megteremtésére és erősítésére egy szerveződésen keresztül, ami lehetne állami, vállalati vagy civil szervezésű is. De egy nonprofit szervezet vagy egyéb szerveződésnél sem feledkezhetünk el az önfenntartásról, de legalább a szükséges költségek csökkentésének lehetőségéről. Ez többféle módon is történhetne.

Egy ilyen szervezet, amennyiben állami szervezésű is, akkor el tudja végezni állam által szükségesnek ítélt, külföldi és belföldi gyártók eszközeinek validálását. Ez csökkenti az állam kiadásait, mivel ezzel nem kell büntetőjogi informatikai szakértőket is alkalmazó cégeket bevonni a kérdéses ügyekben, ha alapból rendelkezésére áll egy ilyen szakembergárda.

Továbbá pénz szerezhető bizonyos rendszerek és eszközök tesztelésével és ellenőrzésével. Mivel, ha egy ténylegesen megbízható és elfogadott szervezet kibervédelmi szempontból pozitívan tud megítélni egy adott terméket, akkor annak komoly marketingértéke lehet egy kibertudatos piacon. Így lehetne különböző védettségjelölések használatát engedélyezni bizonyos gyártók bizonyos termékeinek, amennyiben ténylegesen eleget tesznek a feltételek, és az ilyen tesztelésekért és listába való felvételért eljárási és egyéb, ténylegesen felmerülő költségek megfizetésére lehetne kérni a gyártókat. Így már máris fentarthatóbb lenne egy ilyen szervezet.

Ezekmellett még az emberek kibertérbeli viselkedésének monitorozásával és elemzésével, pl. pszichológusok bevonásával végzett állapotfelméréseket társítani lehet a gépi intelligencia kutatásokkal is. Így nagyobb hatékonysággal dolgozhatunk, valamint uniós és egyéb kutatási alapok megszerzésére is versenybe szállhatunk, ezzel megalapozva egy ilyen szervezet fenntarthatóságát.

Záró sorok

Kutatásom során rengeteget tanultam és rengeteg ijesztő dolgot találtam. De szerencsére nem csak negatív dolgokat sikerült meglelnem. Már most fellelhető a kiberbiztonságra érzékeny emberek csoportja, még akkor is, ha kisebbségben vannak. Jövőbeni célomhoz azt írhatom, hogy megakarom találni azon, hozzám hasonlóan a téma felé nyitott fiatalokat, akik hajlandók tenni a biztonságosabb jövőért. Így velük és már tapasztalt szakemberekkel elindíthatnánk azt a munkát, ami segíthet a jövő technológiáinak megvédéséhez a jelenben, hogy ezen technológiák ne okozzanak nagyobb kárt, mint amennyi hasznot képesek jelenteni, mert ehhez én egyedül olyan kevés vagyok, mint erdőtűzre a vízipisztoly. Már az is hatalmas siker lenne, ha az általam és más, nálam sokkal inkább szakértőbb személyek által javasolt kiberérzékenységet teremtő munka elindulhatna, nem is beszélve arról, ha ennek én is részese lehetnék.

Kutatásom lezárásaként szeretném megköszönni a támogatást a mentoraimnak, valamint a Magyar Innovációs szövetségnek, akik támogatták ezen tanulmány megszületését.