FBI-OS NÉVJEGYKÁ IS VAN VALA

Balra Buttyán Levente, jobbra Bencsáth Boldizsár

RTYÁJUK HOL

A CrySyS Lab nevét előbb ismerték külföldön, mint Magyarországon: felfedezték a Duqut, az egyik leghírhedtebb kiberfegyvert. De nemcsak ezzel foglalkoznak: az autók egymással kommunikálását tették biztonságossá. A tehetséggondozó programjuk pedig már több éve a legnagyobb hekkerversenyre juttatja hallgatóikat.

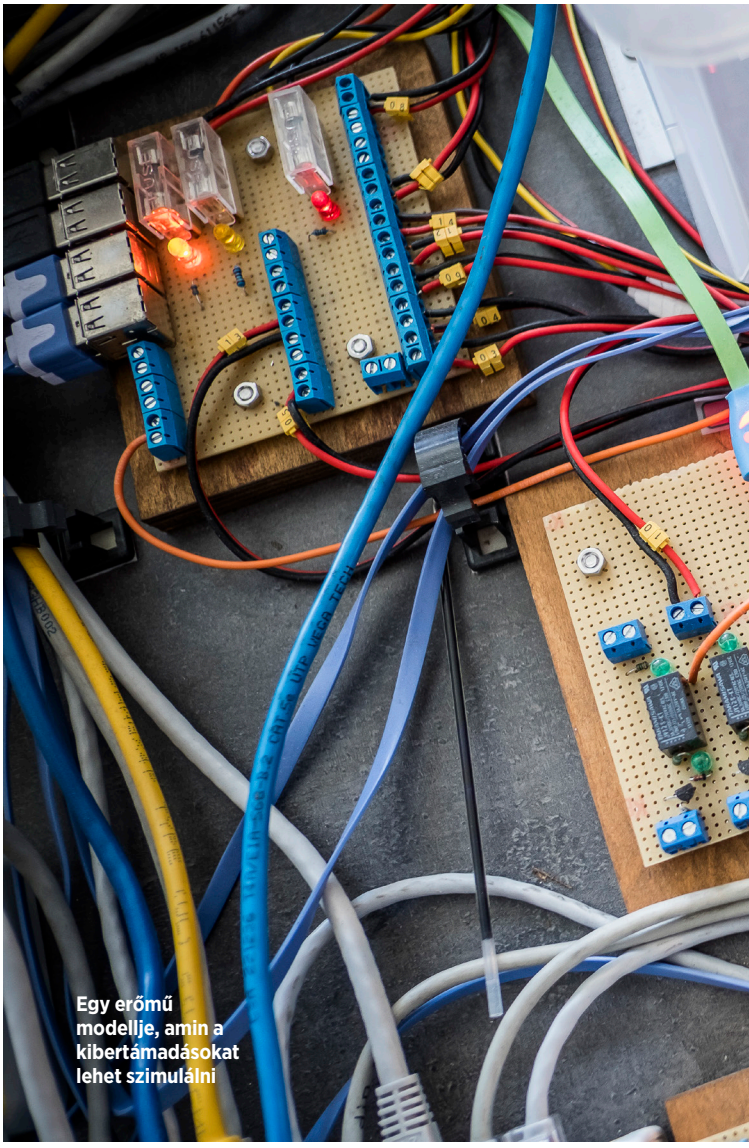
FOTÓK: ORBITAL STRANGERS

ÍRTA: LAZA BÁLINT

Hátul, fel a lifttel - igazít útba a portás, amikor megérkezem a Crysys Labhez, Magyarország nemzetközi szinten talán legismertebb hekkereihez. Nem fancy irodaházban járok a belváros közepén - bár az épülettel semmi gond -, hanem a Budapesti Műszaki és Gazdaságtudományi Egyetem I épületében (sosem fogjátok kitalálni, I = informatika). A történelmi jelentőségű kiberfegyver-leleplezéseket produkáló labor ugyanis nem agyonpénzelt kormánycsatolmány vagy jól jövedelmező magáncég, mint általában a hasonló kaliberű felfedezéseket produkáló közösségek, hanem egy egyetemi labor. Amikor kopogok, éppen arról beszélget Buttyán Levente, a Crysys Lab vezetője és Bencsáth Boldizsár (Boldi), hogyan lehetne javítani a zh-javítások automatizálásán - merthogy több száz van belőlük -, amin éppen dolgoznak (a hallgatóknak választani kell 4 válaszból, a megfelelő betűt besatírozni, ennek felismerésével javítja a gép a dolgozatokat).

„A BME Villamosmérnöki és Informatikai Karon vagyunk, azon belül a Hálózati Rendszerek és Szolgáltatások Tanszéken. Itt tanszékek az egységek, egy tanszék egy tématerületre fókuszál, a miénk a hálózatokra. A tanszéken belül több kisebb csoport van, amiket laboroknak hívunk, ezek a hálózatok különböző aspektusait vizsgálják, mi a biztonsággal foglalkozunk" - mélyedünk bele pillanatok alatt az egyetemi hierarchiába Buttyán Leventével. Az egész karon ők viszik a biztonsághoz kapcsolódó témákat az oktatás és kutatás területén is (nagyjából tucatnyian). Külsős munkákat is elvállalnak, ha felkéri őket valaki, de nem ez a fő tevékenységük.

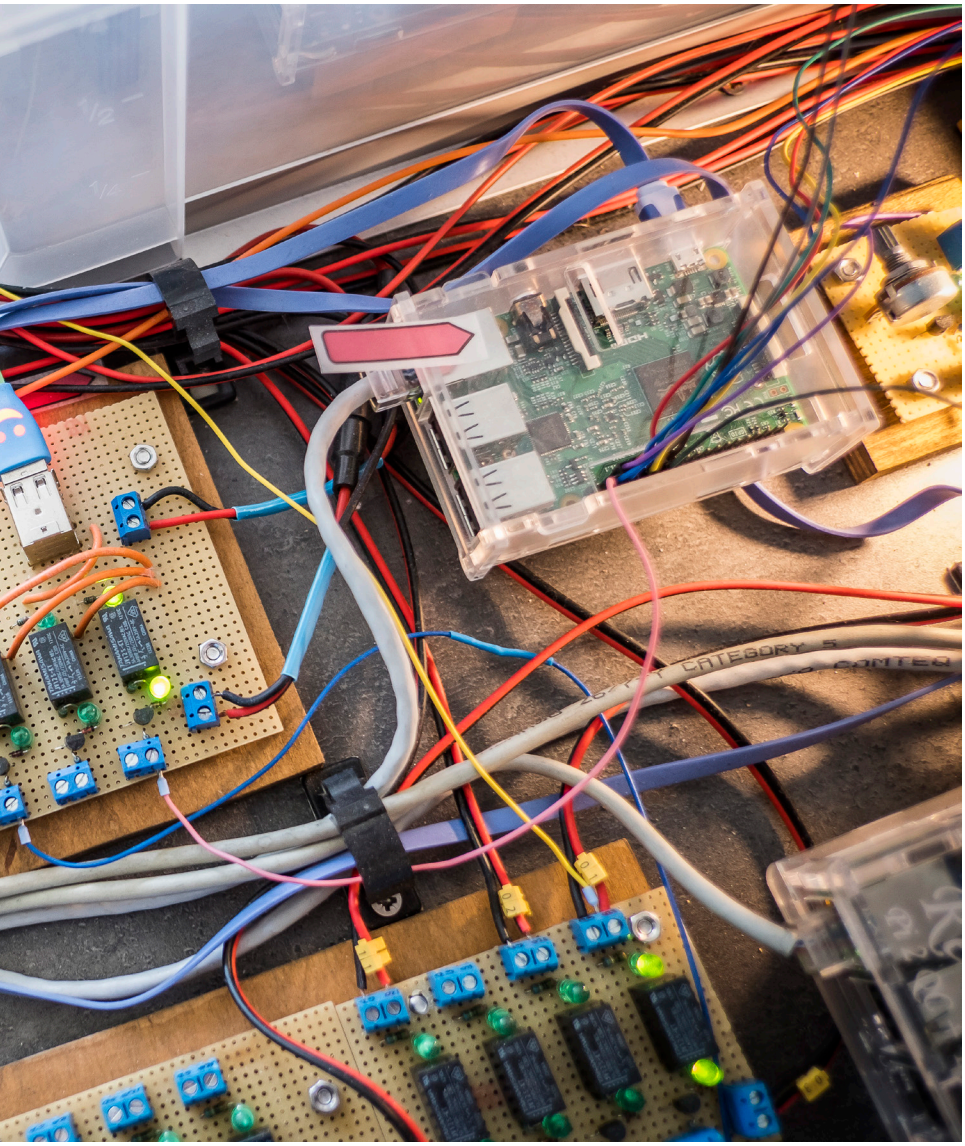
„A legtöbben a Duqu felfedezéséről ismernek minket, pedig nemcsak ezzel foglalkozunk" - mondja Levente. Az ismernek minket valójában enyhe kifejezés: 2011-es felfedezésekor itthon még nem szólt olyan nagyot a téma, az átlagember nagyjából először találkozott azzal, hogy a kibertérben bizony háború folyik, ahová kifejezetten fejlesztenek kiberfegyvereket. Külföldön hatalmasat robbant a találat. A Duqu is ilyen fegyver, nevét az általa létrehozott DQ kezdetű fájlnevekről kapta, a szóról kiderült, hogy franciául azt jelenti: seggből kifelé, a „hasamra csaptam" magyar szólás értelmében - ezért a francia híradókban mindig dukjúnak ejtették. Boldizsárék szerényen mesélnek a fogadtatásról, pedig akkor sokan megjegyezték a kis magyar egyetemi labor nevét, tagjaiknak előre köszönnek a konferenciákon. „Tavaly volt egy konferencia, kimentem vécére. Kinyitottam az ajtót, becsapódott, nagyot koppant. Mondom, sorry. Kikiabál valaki: What sorry? Hangos volt az ajtó, az a sorry. Ja, te azt megteheted, te találtad a Duqut" - meséli a hatását felfedezésüknek Boldizsár.



Egy erőmű modellje, amin a kibertámadásokat lehet szimulálni

VELÜK LÉNYEGÉBEN MINDIG MINDEN PÉNTEKEN TÖRTÉNIK.

A Duqu hasonlóan kifinomult, és bár egyértelmű rokonságot mutat a világon elsőként megtalált kiberfegyverrel, a Stuxnettel, a célja más volt: pontosan nem tudni mi, de nem ipari létesít-



ményeket tett tönkre, hanem adatokat lopott el, ahonnan csak tudott. A Crysys kutatói itt Magyarországon fedezték fel: ma már tudható, hogy a Netlock nevű, biztonsági tanúsítványokat készítő cégnél bukott le, de világszinten bevetették.

A felfedezés jelentőségét jól mutatja, hogy azóta könyvfejezet is született róla, Kim Zetter, kiberbiztonsági szakújságíró a Countdown to Zero Day című könyvében azt írja: „Boldizsár éppen a monitorát bámulta és beleharapott szendvicsébe, amikor megcsörrent a telefon” – a Netlocknál már rájöttek, hogy valami probléma van, segítséget kértek.

A cégnél hamar megtalálták a kiberfegyver billentyűzetfigyelő része által rögzített adatokat (keylogger). „Hogyan vettem észre? Megnéztem, mi van az ideiglenes könyvtárakban és volt egy fájl, aminek nőtt a mérete. Gépeltem pár betűt, nőtt a mérete – nem írtam, nem. Nem őrületes technológia van mögötte” – meséli Boldizsár gépelést imitálva az asztalon.

A Duqunak volt egy másik trükkje is: csak a gép negyedórás inaktivitása után telepítette magát, így aki kereste a gépen a fertőzést, nehezen találta meg. Boldizsár is úgy fogta meg, hogy elindította virtuális gépét, hogy megfertőzze – akkor már megvolt, melyik fájl a hunyó –, de nem történt semmi. Hazament vacsorát főzni (minden este ő főz), és mikor távolról ránézett a virtuális gépre, jelzett a rendszer, egész pontosan világított, mint a karácsonyfa: megfertőződött.

„Először név nélkül ment ki ez a publikáció a Symantec anyagában, utána vállaltuk a saját nevünkkel is, de sokaknak fura volt, hogy mi ez a labor” – meséli Boldizsár. „Mindenféle szervezetek próbáltak kapcsolatba lépni velünk, mint például a BBC, akik először kerestek egy magyart, akivel megkérdeztették, tudunk-e angolul, de a US Certtől is írtak emailt, hogy néhány kérdést feltennének” – mondja. A US Cert az amerikai kiberbiztonság (egyik) csúcsszerve, biztonsági információk megszerzésével és elosztásával foglalkoznak. „Megkérdezték, hogy hol hívhatnak, a vezetékes telefont adtuk meg, itt ültünk az asztalnál” – aztán miközben beszéltek, Boldizsár telefonja megcsörrent, de a szám csak annyi volt: +12337, ami nagyon hasonló az 1337 számhoz, azaz „leet”, ami egy speciális írásmód, hekkerkörökben divat használni. Erre azóta sincs biztos magyarázatuk, tippjük szerint így ellenőrizték, hogy Boldi valóban a szobában van, hiszen nem tudhatták, a vonal másik végén kivel beszélnek.

A VILÁG LEGNAGYOBB HEKKERKONFERENCIÁJÁRA JÁRNAK

Bár Boldizsár beszélgetésünk egy pontján viccesen megállapítja, hogy velük lényegében mindig minden pénteken történik, én csütörtökön érkeztem hozzájuk, egyáltalán nem véletlenül: ezen a napon tartják ugyanis az úgynevezett Student Core összejöveteleket. „Külön foglalkozunk tehetséggondozással. Nem lenne kötelező, csinálhatnánk azt is, hogy leoktatjuk a tárgyainkat, és kész” – mondja Levente.

Az egyetemen a diákok tankörökbe rendeződnek, ezeknek rendszeresen tartanak alkalmakat, amikor 40–50 percben elmesélik, mit csinálnak, megpróbálják felkelteni az érdeklődésüket. És miden évben rendeznek egy házi versenyt, úgynevezett SecChallange-t: ez egy hekkerverseny, ahol a diákok kipróbálhatják magukat különböző feladatokon, biztonsági réseket kell megtalálniuk, bejutniuk rendszerekbe, gépekbe. Az itt kitűnő diákokból áll össze a Student Core.

„Ez egy önképző kör. Nincsenek formális előadások, mindenki valamilyen szinten valamilyen témakörhöz ért, abban el is mélyed nagyon, profivá válik. Egymást oktatják az ott levő emberek. Meg versenyekre készülnek” – magyarázza Levente. A programjuk, úgy néz ki, bejött: az önképzőkörből alakult !SpamAndHex nevű hekkercsapat már sokadszorra jut be a DefCon CTF (Capture The Flag)

döntőjébe. Aki nem mozog hekkerkörökben, annak nem sokat mond ez a név: a DefCon a világ legnagyobb hekkerkonferenciája, az itt rendezett versenyekre a kiberbiztonság-hekkelés területén kiemelkedőnek számító államok, mint Kína, USA, Dél-Korea állami támogatásokat nem kímélve delegálnak csapatokat, mert aki itt nyer, azt világszinten jegyzik.

A magyar srácok pedig magukat képzik, és támogatóktól, apránként, nem könnyen kalapozzák össze az utazáshoz szükséges pénzt. A DefCont ugyanis Las Vegasban tartják. Ez az a konferencia, ahol a különböző hárombetűs ügynökségek emberei árgus szemekkel figyelnek, az előadók sokszor nekik is új technikákat, biztonsági réseket mutatnak be, az ott látottak meghatározhatják a következő évek hekkelési trendjeit. A Student Core-ba visszajárnak az „öregdiákok" is, segítik a tehetséges, de még diák tagok felzárkózását, amíg idejük engedi. A kör létszáma ezzel stabilan nagyjából 15 fő.

Idén is sikeresen behúzták a DefCon döntőjét, de nincsenek elszállva maguktól. Pedig lenne mire. Ez tényleg világszinten csak pár csapatnak sikerül, de ők inkább elkezdik átbeszélni a várható feladatokat és szervezik, hogyan jutnak majd ki a döntőbe, honnan lesz rá pénz.

Ebbe gyűlnek a sokszor beazonosíthatatlan vendégek és hárombetűs ügynökségek névjegyei

AUTÓ + HEKKER = BALESET

Nemzetközi ismertség ide, Duqu oda, a Crysys alapvetően egyetemi környezetben működik, ahol kutatásokkal is kell foglalkozniuk. Ebben pedig témájukat nem a kiberfegyverek adják - az csak később jött az életükbe -, hanem a kiberfizikai rendszerek biztonsága: ezekben számítógépes rendszer felügyel vagy vezérel fizikai folyamatot, és a kiberoldalról érkező támadásoknak lehet fizikai hatása. A világon először felfedezett kiberfegyver, a Stuxnet is lényegében ez a terület: az iráni urándúsító centrifugákat szoftveresen tették tönkre vele.

A kutatói közösségben erről voltak korábban ismertek. „Emiatt, amikor a Duqut megtaláltuk, az első értesítéseket nemcsak a nagy cégeknek, mint a Microsoft vagy a Symantec küldtük ki, hanem kutatóknak, mert oda jobb kapcsolatunk volt, és azt gondoltuk, hogy a nagy cégek nem tudják, hogy kik vagyunk, majd a kutatók segítenek bejutni a nagy cégekhez. De nem ez történt, pont az ellentéte: a kutatók nem csináltak semmit, a nagy cégek meg rögtön válaszoltak" - meséli Boldizsár, aki közben is csinálja dolgát a számítógépén.

Az ipari rendszerek biztonsága mellett egy egyre égetőbbé váló problémával is foglalkoznak: az autók kommunikációjával. Az önvezető, vagy csak simán okosautók kommunikálni fognak egymással és így sokszor jobban döntenek, mint az ember. Ha a kocsik tudnak egymásról, elkerülhetők lehetnek balesetek, de könnyebb lehet egy egyszerű sávváltás is. Kár, hogy a dolognak van másik oldala is: ha valaki befolyásolni tudja a kommunikációt, rosszindulatú üzeneteket adhat ki a kocsinak, és a támadásnak akár

EXTRÉM ESETBEN NEM ÁTLAGEMBERT KÖVETNEK, HANEM A MINISZTERELNÖKÖT KÖVETHETIK VÉGIG AKÁR TERRORISTÁK.

baleset is lehet a vége.

Nem ma kezdték, 2006 óta foglalkoznak a területtel, európai uniós projektek keretében. „Elég sarkalatos véleményem van az úniós projektekről, doktori kutatást kivéve ritkán lesz belőlük bármi" - mondja Levente, ez a projekt viszont kivétel volt: amit akkor megalkottak, ma már az egymással kommunikáló autók ipari szabványának része.

Iránban kezdődött az új hadviselés

A Duqu hatalmas jelentőségű volt, a világ még éppen csak felocsúdott a Stuxnetből: utóbbi kiberfegyver új minőséget hozott, a ma elérhető információk alapján valószínűleg amerikai-izraeli együttműködésben készült, kifejezetten azért, hogy hátráltassa Irán atomprogramját. A natanzi atomlétesítménybe bejutva tönkretette az urándúsító centrifugákat (magasabb fordulatszámon pörgette őket a kelleténél, miközben a monitorra azt írta, minden rendben), ezzel egy ideig mindenképpen akadályozta az iráni atomprogramot.

Leventéék azzal foglalkoztak, hogyan lehet egyszerre biztonságossá tenni az autók kommunikációját, kiszűrni a rosszindulatú támadókat, és a magánéletünkből is megőrizni valamennyit, még ha ezek ebben az esetben egymásnak ellentmondó kritériumoknak is tűnnek. Ugyanis a biztonságra az a megoldás, hogy az autók minden egyes üzenetét aláírják úgynevezett kulcsokkal, így a fogadó autó tudja, hogy amit kap, az hiteles. Viszont, ha mindenkinek egyedi az aláírása, akkor ez alapján már könnyen beazonosítható. „Extrém esetben nem átlagembert követnek, hanem a miniszterelnököt követhetik végig akár terroristák" - magyarázza Boldizsár.

A megoldás az lett, hogy az autók több kulcsot kapnak, amit váltogatnak. Ez alapján még követhető lenne bárki, mert, ha megy egy úton egyedül, egyszer csak kulcsot vált, és előtte tudtuk az irányát és a sebességét, akkor egyértelmű, hogy akit pár méterrel arrébb látunk üzeneteket küldeni, az még mindig ugyanaz az autó. A megoldás: amikor sok autó találkozik, mondjuk egy kereszteződésben, egy pillanatra elhallgatnak, egyszerre cserélnek kulcsot, így már nem egyértelmű, hogy végül is ki merre ment tovább.

KÜLFÖLDI JÓ GYAKORLATOK

De hogyan lett egy egyetemeken megszokott, kutatásokkal foglalkozó laborból egy nagyon gyakorlatias, nyertes hekkercsapatokat nevelő és állami kiberfegyvereket lebuktató szellemi műhely? „Az egész úgy kezdődött, hogy a kilencvenes évek közepén, amikor én idejártam egyetemre, nem nagyon volt még adatbiztonsággal foglalkozó tárgy, hanem egyetlen professzor volt, aki a kódolástechnika keretein belül beszélt kriptográfiáról. Vajda István tanár úr, most is itt dolgozik a laborban" - meséli a kezdeteket Levente. „Én voltam az első doktorandusz, aki ezen a tanszéken biztonsággal kezdett foglalkozni" - mondja. A kriptográfiában nem látott nagy perspektívát, mert ilyen titkosító algoritmusokat világszerte csak pár száz ember tervez, a többiek csak használják őket, nagyon szűk a terület. Ezért gyakorlatiasabb irányba fordult, hálózatbiztonsággal, protokollok tervezésével kezdett foglalkozni, majd kapott egy lehetőséget, és kiment Svájcba, a lausanne-i műszaki egyetemre (EPFL) tanulni. „Boldival akkor még nem is találkoztunk, ő pont ekkor jött a tanszékre" - mondja. Akkoriban egy cég támogatásából már elkezdett felépülni a labor elődje, de igazán akkor indult be, amikor Levente visszajött.

„A kinti lét nagyon meghatározó lett, az egész tudományhoz való hozzáállásuk, szemléletük miatt. Az EPFL európai szinten top iskola, átvették az amerikai mintát. Pezsgés volt, jöttek-mentek a meghívott vendégek, mindig volt valami szeminárium, amire be lehetett ülni és be is ültek az emberek" - meséli. „Itt sokkal több mindennel kell foglalkozni, sok apró projekt van, hogy meglegyen az a pénz, amiből meg lehet élni, ezért az embernek nincs ideje, hogy beüljön mondjuk egy szemináriumra. Ott kint egy–két nagy projekt ellátta az egész labort, mindenki nyugodtan dolgozott, bele tudott mélyülni, minőségi munkát tudott csinálni" – mondja. Ez látszik a délutáni labormeetingen is, amit végighallgattam: pont félévet összegeznek, és megjegyezni sem könnyű, mennyi projekten dolgoznak; röpködnek a rövidítésekből álló nemzetközi és magyar projektnevek, például H2020, VKE, VKE2. Rengeteget kell pályázniuk, ami sok adminisztráció, de végül csak a pályázatok egy része sikeres és hoz pénzt is.

A sokfelé szakadás nagy terhelést jelent. „A márciusom úgy nézett ki, hogy elutaztam Hawaiira, ott voltam pár napig, visszafelé még megálltam Kanadában egy megbeszélésre, hazajöttem. A következő héten hétfőn-pénteken mérést tartottam, kedden és szerdán oktattam, szombaton mentem vissza a Karib-térségbe, 27 óra volt, a két utazás alatt 11 különböző repülőn ültem. Ezalatt három előadásomat kellett itt pótolni, saját feladataim felhalmozódtak, május elejére nemhogy a végére nem értem, hanem elkezdhettem a feltorlódott dolgok egy részét feldolgozni. Gyakorlatilag az egész félévem arra ment rá, hogy elmentem két meghívásos konferenciára. Az ottlétem mégis kritikus, mert ott tudok csak

Ha valaki magyarul ír diplomatervet, az azt jelenti, hogy örökre rejtjelezi azt.

találkozni olyan kutatókkal, akikről ti írtok utána cikket" – szemlélteti a problémát Boldizsár.

HÁBORÚ VAN, PÉNZ NINCS

„Egy magyar adjunktus fizetése 253 ezer forint bruttó, szükségünk van projektekre, hogy ezt ki tudjuk pótolni. Ott kezdődik az egész, hogy az alapfizetésekre sem kap elég pénzt a tanszék, és odáig tart, hogy a BME nem vehet számítógépet" - mondja Levente. Beszerzési stop van, az egyetem költségvetési intézmény. „Az senkit nem érdekel, hogy informatika karon mégis hogy oktassunk számítógép nélkül. Mobilt sem lehet venni. Azt megértem, hogy ne vegyünk mobilt magunknak, de manapság nem mobilon kellene dolgokat kipróbálniuk a diákoknak?" - teszi fel a kérdést.

A VILÁGON ELŐSZÖR FELFEDEZETT KIBERFEGYVER, A STUXNET IS LÉNYEGÉBEN EZ A TERÜLET: AZ IRÁNI URÁNDÚSÍTÓ CENTRIFUGÁKAT SZOFTVERESEN TETTÉK TÖNKRE VELE.

„Nézd meg azt a nyomtatót, nem a miénk, nem véletlenül van rajta matrica, kölcsönbe kaptuk" - mutat rá Boldizsár. „Volt már arra lehetőségünk, hogy az egész labort elvigyük innen egy külföldi országba, de nem éltünk vele. Konkrétan olyan összegeket mondtak, amivel egy év alatt egy életre elegendő pénzt kerestem volna" - mondja. De nem ezért csinálják, úgyhogy maradtak.

Pedig az utánpótlásképzés nem egyszerű, és a cégek - bár azért rendszeresen jelentkeznek, hogy adjanak nekik kiváló munkaerőt - támogatásra már ritkán gondolnak, ha pedig igen, a kis vállalkozásoknak nincs ehhez elég pénzük, a nagyoknál pedig nehezen megy át a bürokrácián a dolog. „Ez az én dobozkám, ebben azokat a névjegykártyákat tartjuk, akik meglátogattak minket. Két lényeges dolog van benne: az egyik az, hogy láthatóan nagyon sokan jönnek, a világ minden tájáról, még FBI-os névjegykártyám is van valahol. De ez csak egy része, csomóan nem adnak névjegykártyát, főleg olyan szervezeteknél." Ebbe a dobozba kerülnek azok is, akik mindenfélét ígérnek, támogatás végül nem érkezik, csak kérnének. „A DefCon döntőjére tavaly 8 embert utaztattunk, egy jegy akkor 470 ezer forint volt" - egyenként kellett összeszedni.

„Amikor Levi visszajött, elkezdett bevezetni olyan apró változásokat, amik fel sem tűntek itt. Most már persze feltűnő, hogy egy másik labor nem úgy csinálja. Nagyon egyszerűekre gondolj, hogy elmegyünk közösen ebédelni, közben beszélgetünk, szinkronizáljuk, ki mit csinál. Ilyen nem volt, mindenki összevissza csinált valamit" - mondja Boldizsár. A

másik ilyen dolog az volt, hogy az előadásaikat, diplomaterveket elkezdték angolul készíteni.

„Nem gond, ha szarul van megírva angolul. Még mindig jobb, mintha tökéletes magyarsággal van megírva” - mondja Boldizsár. Ha valaki magyarul ír diplomatervet, az azt jelenti, hogy örökre rejtjelezi azt. Senki nem fogja elolvasni, maximum 10 millióan. A 8 milliárdból” - szemléleti Levente a problémát. „Meg voltam arról győződve, hogy tudunk csinálni mi is nemzetközi publikációkat” - mondja. Publikációkban jól is állnak, jó az idézettségük, de úgy érzik, ezt fenntartani sokkal nehezebb itt, mint máshol.

„Itt az adatbiztonság területén ez a bezártság teljesen jellemző. A kutatók nem azzal foglalkoznak, mikor utaznak külföldre, összehasonlítani a munkájukat másokkal. Nem abban gondolkodnak, hogy nemzetközi szinten egyenlő minőségűek vagyunk az amerikai top kutatókkal vagy a dél-koreaiakkal, hanem mindig bezárva Magyarországon én jobb vagyok-e, mint valamelyik másik magyar” - erősíti meg Boldizsár.

Próbáltak ezen változtatni: „Ha itt járt nálunk egy külföldi, mindig szerveztem szemináriumot, mert azt láttam, hogy kint is így csinálják - ha már idejött ez az ember, és fizetni sem kell érte. És az egyetemi emberek szeretnek beszélni arról, amit csinálnak” - mondja. Itthon azért nem ment ilyen jól a dolog, kevesebben jöttek el az így szerveződő előadásokra, hiába hirdették meg azokat, Levente szerint pont a túlterheltség miatt.

Figyelnek arra is, hogy a doktoranduszok minden védésénél az egyik bíráló magyar, a másik külföldi legyen. „Sokkal nehezebb megszervezni, más nem is nagyon csinálja. Volt olyan, hogy mi fizettük ki az útiköltségét, de idejött, bírált” - meséli Levente. Fontos nekik a publikációk nyelvi minősége is. „Svájcban volt olyan anyanyelvi angol, akinek csak az volt a feladata, hogy nyelvileg javítsa mindenki cikkét” - itt erre nincs lehetőség, maguknak kell figyelni rá.

Levente 2003 januárjában jött vissza, és a labor felfuttatásához volt egy kis szerencséjük is: 2004-ben Magyarország belépett az EU-ba, elkezdték megkeresni külföldi partnerek. „Ott konkurens voltam, itt lehetőség” - mondja nevetve. Mivel mások innen nem publikáltak külföldre, csak őket ismerték, egyből négy uniós projektet is behúztak. „2011-ben a Duqu óriási változás volt. Tök jó volt, hogy Boldi gyakorlatorientált, kevesebbet publikál, de nagyon ért minden rendszerhez, ő itt tudott maradni. És beért, hogy ez is egy érték” - mondja Levente.

Itt sokkal több mindennel kell foglalkozni, sok apró projekt van, hogy meglegyen az a pénz, amiből meg lehet élni, ezért az embernek nincs ideje, hogy beüljön mondjuk egy szemináriumra.

Spinoffok

1. A Crysys Labből több cég is indult. Ilyen például a Tresorit, aminek az alapja két hallgató, Lám István és Szebeni Szilveszter TDK-dolgozata és diplomamunkája volt. Buttyán Levente volt a konzulensük, emiatt tiszteletbeli alapító-tulajdonos is a cégben, kis százalékkal. A Tresorit biztonságos Dropbox-alternatívát kínál, a felhőben tárolt fájlokat úgy titkosítják, hogy ahhoz a tárhelyszolgáltató sem férhet hozzá.

2. Az Avato egy olyan webes alkalmazás, ahol IT-biztonsági feladatokat lehet megoldani. Az egyetemi élet inspirálta, nagy, 450 fős tárgyakhoz nehéz gyakorlatot csinálni, így viszont mindenkinek tudnak feladatokat adni. Több mint 400 feladat van benne, sokféle témakörben, használják versenyekre is, de van már olyan cég, amelyik előfizetett rá, így képzi alkalmazottjait. Ehhez a startuphoz most keresnek befektetőket, egyelőre hallgatók dolgoznak rajta.

3. A Ukatemi Technologies-ben Levente és Boldizsár tulajdonosok, négy alkalmazottjuk van. Üzemeltetnek itt például malware repositoryt: feltöltik az összes kártékony kódot, amit találnak, vagy máshol már elérhető, hogy naprakész adatbázisuk legyen helyben. Ha egy céget támadás ér, könnyebben tudják beazonosítani, miről van szó. A másik szolgáltatásuk, hogy vizsgálják a mások által beküldött gyanús weboldalakat: automatizáltan virtuális géppel meglátogatják őket, és megpróbálják megfertőzni, ehhez pedig mindent rögzítenek, így vissza lehet pörgetni, mi történt, ami például a vírusirtó gyártóknak nagyon hasznos.