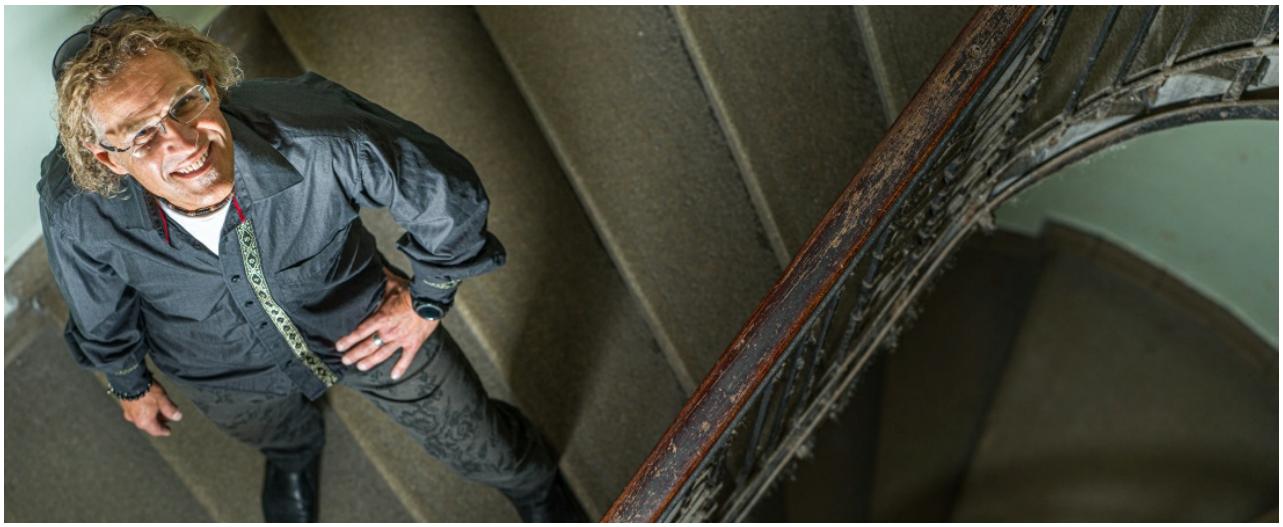
IT-biztonsági szakértő: Jártam olyan kórházban, ahol még XP meg Windows 95 futott – tavaly

forbes.hu/legyel-jobb/csizmazia-darab-istvan-eset-sicontact-antivirus-blog-interju-kiberbiztonsag

2020. június 23.



2020. június 23.

Csizmazia-Darab István az ESET antivírus egyedüli hazai partnerének számító Sicontact Kft. IT-biztonsági szakértője, ezen felül pedig a 13 éve futó Antivírus blog házigazdája. Az IT-újságírásban csak Rambóként ismert szakember dolgozott szobaméretű számítógépekkel, hackelt Commodore-on, éveket töltött víruslaborokban, és megannyi előadásban és cikkben próbálta rávenni a nagyérdeműt a lehető legteljesebb online védekezésre, legyen szó egy jó kis antivírus-program telepítéséről, vagy akár egy, az 1234-nél erősebb jelszó implementálásáról. Nem szereti a távinterjúkat, tíz éve van home office-ban, találkozásunkkor pedig azonnal kezet nyújt – hiába, a számítógépes vírusoktól a kézfertőtlenítő sem véd meg. És akkor az olyan legenda, mint hogy a Mac vagy a Linux vírusmentes, még szóba sem került. Nagyinterjú.

***

Mondtad, hogy nem annyira szeretsz interneten kommunikálni. Ez szakmai ártalom?

Nem, rendben van az internetezés. Nemrég olvastam a Tizenhárom almafa című könyvet Wass Alberttől, ami a székelyekről és az ő helytállásukról szól. Az apai nagyanyai ágam székely. Nekem tetszik az ő gondolkodásuk, ami szerint akkor tudunk igazán beszélgetni, ha egymás szemébe tudunk nézni. Lehet videokonferencia is, de ha választani lehet, az élő kontaktust preferálom. Telefonálni nem is nagyon szoktam.

Mondhatnám, hogy a karanténidőszak nehéz lehetett, de e-mailben azt írtad, tíz éve home office-ban vagy.

Ez így van.

Ez nem elidegenítő?

Kicsit autista beütésű vagyok. Lehet, ezt még fel se találták, amikor én megszülettem, lévén mindjárt hatvanéves leszek. *(Nevet.)*

Ezt mondjuk nem gondoltam volna.

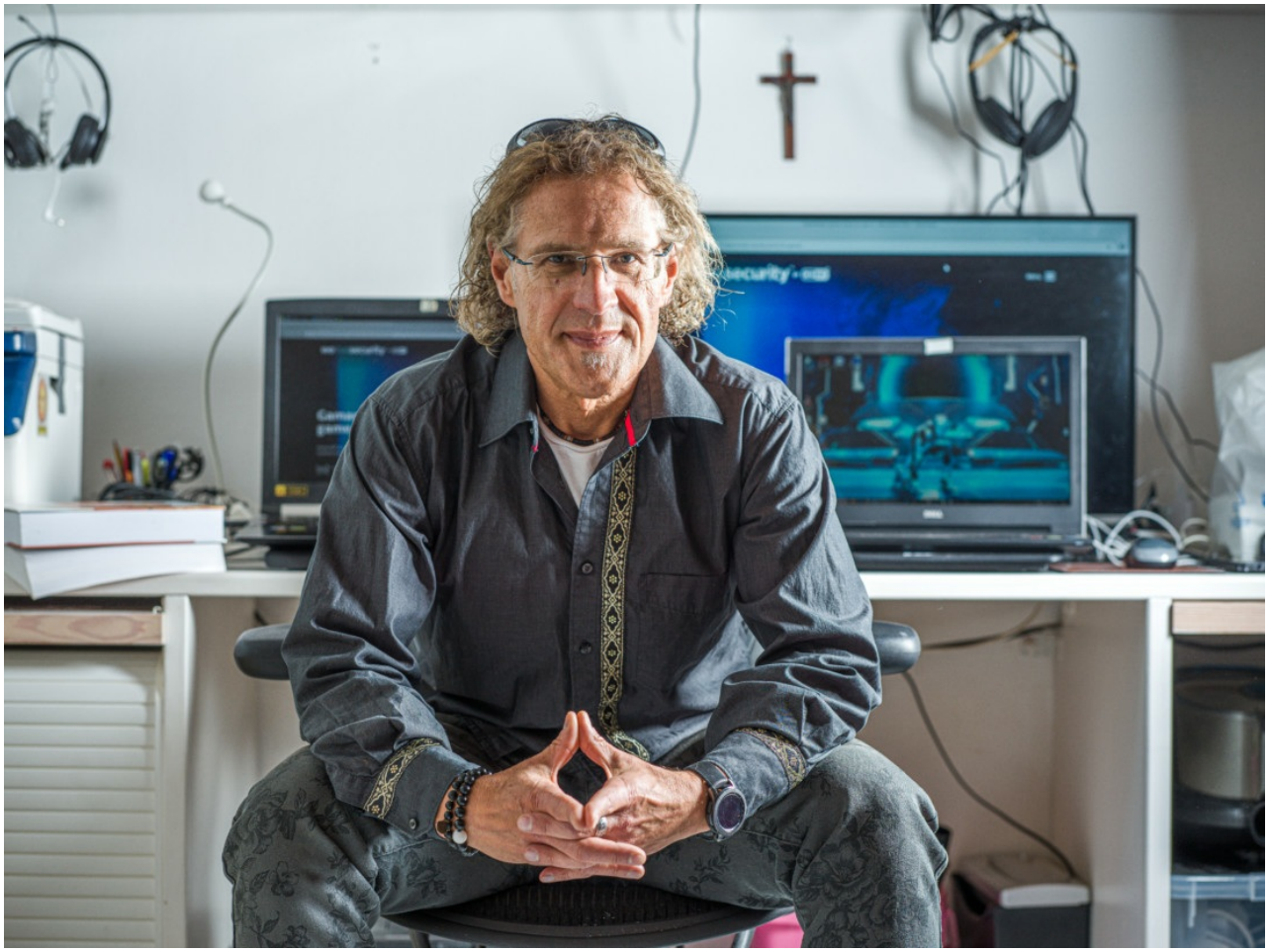
Elég feladatorientált vagyok. Van egy listám, rajta minden, amit el kell végezni. Nagyon hálás vagyok, ha nem zavarnak közben. Egyébként programozóként kezdtem, 1988-ban volt az első programozói munkahelyem, a Volán Tefu. Wáberer György volt a számítástechnikai osztály vezetője.

Nahát.

Aztán jött a másik nagyvállalat, az Erőterv, itt 11 évig mérnöki támogató munkát végeztem. Már akkor jöttek a vírusok, kineveztek a munka mellett vírusvédelmi felelősnek egy négyszáz gépes hálózatba. Mindenki utált dokumentumokat írni az Erőtervben, ahol elég nagy szigorúság van, mindent le kell dokumentálni, kicsit a repüléshez hasonlít. És hát, amikor tudták, rám testálták ezt.

Te nem utáltad?

Elvoltam vele, elbabráltam. Később kifejezetten szerettem.



Csizmazia-Darab István, alias Rambo, az egyszemélyes antivírus-hadsereg, háttérben az arzenállal. Természetesen az összes gépen fut vírusirtó. István régebben retro-számítógépeket is gyűjtött, de sokat költözött, így egykor legendás gyűjteménye már nincs meg, eladta // Fotó: Sebestyén László

Honnan van a beceneved?

1984-ben vonultam be katonának és akkor volt egy műszaki bizományi a Majakovszkij utca sarkán. Árcsökkentés volt, 100 ezer forintról 64 ezerre csökkent a Commodore 64-es alapgépnek az ára. Ebben az időben a Merkúrnál Trabantra 60 ezerért, Zsigulira 72 ezerrel lehetett előfizetni, színválasztás nélkül, mert az plusz ötezer lett volna. Csak hogy értsd, ez mekkora befektetés volt akkoriban.

> A bátyám rendszerszervező volt az Autokernél, így nagygépes környezetben is tettem látogatást, 1980-ban pedig R20-R40 operátorként is dolgoztam, de mégiscsak a Commodore lett az első számítógépem.

Egy ideig lekötöttek a játékok, aztán elkezdtem hackelgetni, kimenteni adatokat, képeket a játékokból. Régen volt egy aktívabb klubélet, én az ELTE Homelab számítógép-építő klubba jártam. Mindenféle elborult programozó oda jött.

Abban a közegben mindenkinek lett egy beceneve, alkotói nickje, amit magának választott. Akkor ment mozikban az első Rambo, ami nekem nagyon tetszett, és testhezállónak is éreztem. Dolgoztam csapatban, mikor nagyvállalati programozó

voltam, de elég hamar eljutottam abba a fázisba, hogy megbíztak valami programmal, békén hagytak, aztán szóltam, amikor kész voltam – egyedül tudtam a leghatékonyabban dolgozni, one man force-ként.

Ma is szólítanak így?

Igen, a szakmában.

Hogy jöttek képbe a vírusok?

1988-ban, mikor az első jelentős potyogós vírus felbukkant a Számalkban, ahová jártam, akkor jelent meg az első vírusvédelmi cikkem is a Computerworld című magazinban, a Mester Sándor-féle újságban. Később víruslaborban és vírusvédelmi cégeknél is dolgoztam. Én lettem az a hibrid, aki ért is a vírusokhoz, és tud, sőt szeret írni róluk. Mert a marketinges is tud írni, csak nem érti, mit mondanak neki a laborban. A laboros meg azt mondja, hogy hagyják békén, ő elbitvadászkodik, de írjon erről valaki más. Én hosszú távon szívesen töltöttem be ezt a szerepet már több munkahelyen is.

Vírust írtál valaha?

Nem.

Nem is jutott eszedbe?

Ez erkölcsi kérdés számomra. Fontos nekem a becsületes hozzáállás, ez a buddhizmusból is visszaköszön. A vírusíró elég okos ember, de miért nem alkalmaznak vírusírókat a vírusirtó cégek?

Miért nem?

Mert az erkölcsi mércét nem ütik meg ezek az emberek.

> Itt egyszer lehet eljátszani a becsületedet.

Hogy tudtad beindítani a karrieredet? A vírus relatíve új jelenség volt, a legtöbb ember nem tudta, hogy a hétköznapjaikba be tudnak ezek furakodni.

Hát, a vírusok azért elég régi dolgok. A vírustörténelmi nulla kilométerkövet 1986-ra teszik. Korábban is voltak már vírusok, de széles körben a Brain vírus terjedt el először. Ötnegyed colos IBM XT kompatibilis gépek floppy lemezein terjedt nagy tömegben. Pakisztánban írták, nem tetszett az ottani fejlesztőknek, hogy lopják a szoftvereiket, ezt amolyan kis büntetésnek szánták. De a készítők beleírták a nevüket, címüket és telefonszámukat is. Akkoriban ez más világ volt. Commodore 64-re is volt egyébként vírus, ami floppyról floppyra terjedt, maga a gép 1982-ben jelent meg Amerikában, 1983-ban pedig Európában. Vírusirtót is írtak már Commodore-ra.

Visszaemlékezve a munkahelyre, még a Volán Tefu annyira nem volt necces, egyszer-kétszer fordult elő fertőzés. Az Erőterv már keményebb volt, határidők, külföldi vagy belföldi partnercéggel kijelölt haladási mérföldkövek voltak, így ha állandóan lefagyott egy gép, újraindult vagy letörölt valamit, azt egyszerűen nem lehetett megengedni. Muszáj volt ezzel a kérdéssel foglalkozni, mert akadályozta a munkát. Ki kellett jelölni egy felelőst és gondoskodni arról, hogy menjen a munka – annak is, aki esetleg nem ért a géphez, csak AutoCAD-ezik vagy leveleket ír.

Hogyan kerültek akkoriban vírusok ezekre a rendszerekre? Ma már tudom, hogy kerülnek: ott az internet, jön egy hozzá nem értő kedves alkalmazott, esetleg az IT-s nem foglalkozik vele eléggé. De akkoriban ez hogy volt? Valaki beszambázott egy jó kis kazettával vagy nagylemezzel, hogy hahó, hoztam egy vírust?

Floppylemezen terjedtek, ezeken jelentek meg a vírusok és a vírusirtók is. A 80-as évek elég nagy hőskor volt. Ekkoriban voltak a BBS-ek, nem tudom, ezekről hallottál-e.

Hallottam.

Ez a Bulletin Board System rövidítése. 1200, 2400, 3600 boardos modemekkel tárcsázott be az ember egy ilyen számra, hogy letölthessen róla szoftvereket. Onnan lehetett vírusokat, vagy akár vírusirtókat letölteni. Ehhez képest, hogy hol tartunk most! Megnéztem a héten az AVTest.org statisztikáit, ami egy vírusteszteléssel foglalkozó, megbízható weboldal, ahol nyilvántartják, hogy mennyi az egyedi, kártékony kódok mennyisége összesen. Egymilliárd-ötvennyolcmillió volt a héten.

Nagy utat tettünk meg. A vállalkozások ezt hogyan kezelték az elmúlt harminc évben? Fejlődtek, vagy még mindig ugyanazokat a problémákat látod nálunk, mint húsz éve?

A problémák változók, szerintem a figyelem és az információ már megvan a védekezéshez.

> A vállalkozások méretben elég különbözőek. Ha kkv-król beszélünk, nekik a legsanyarúbb a helyzetük.

Egy nagy cégnél ki van nevezve GDPR-felelős, adatvagyon-szakértő, van biztonsági részlegük, vagy legalábbis külsősökkel megoldják. Kis cégeknél, akik 5-10-20 főből állnak és örülnek, hogy élnek, sokszor el van felejtve ez a dolog. Azok szoktak komolyan törődni vele, akik egy nagy cég partnerbeszállítói. Ezeknél az incidenseknél egy jellemző mintázat, hogy a gyengébb beszállítói kört támadják először: föltörik és megfertőzik őket, majd onnét, mint egy ugródeszkáról indulnak meg az értékesebb célpontok felé.

És a felhasználókkal mi a helyzet? Tudatosabban védekeznek most, mint régebben?

Én úgy látom, hogy javult ez a helyzet. A nagyanyáink még elgondolkoztak rajta, hogy bezárják-e a kertkaput, aztán egyszer jött valami rossz ember és elhajtott egy tehenet, három évig erről beszéltek és ez lett, amire vigyázni kell. Most olyan mennyiségű cikk, információ lát napvilágot vírusvédelem témájában, hogy az emberek általában óvatosabbak lettek.

Mindig van persze olyan, aki azt mondja, hogy oké, egyszer feltelepítem a gépet és többet nem foglalkozom vele. Ő az, aki nem frissít, meg bármit kap a Facebookon, megosztja, el se olvassa. Ilyen jelenségekkel mindig fogunk találkozni, de úgy látom, sokan felkapják a fejüket ezekre a dolgokra és igyekeznek más kárán tanulni. Látszik a fejlődés, olyan kérdésekkel érkeznek, amiken érezni, hogy már utánaolvastak a témának.

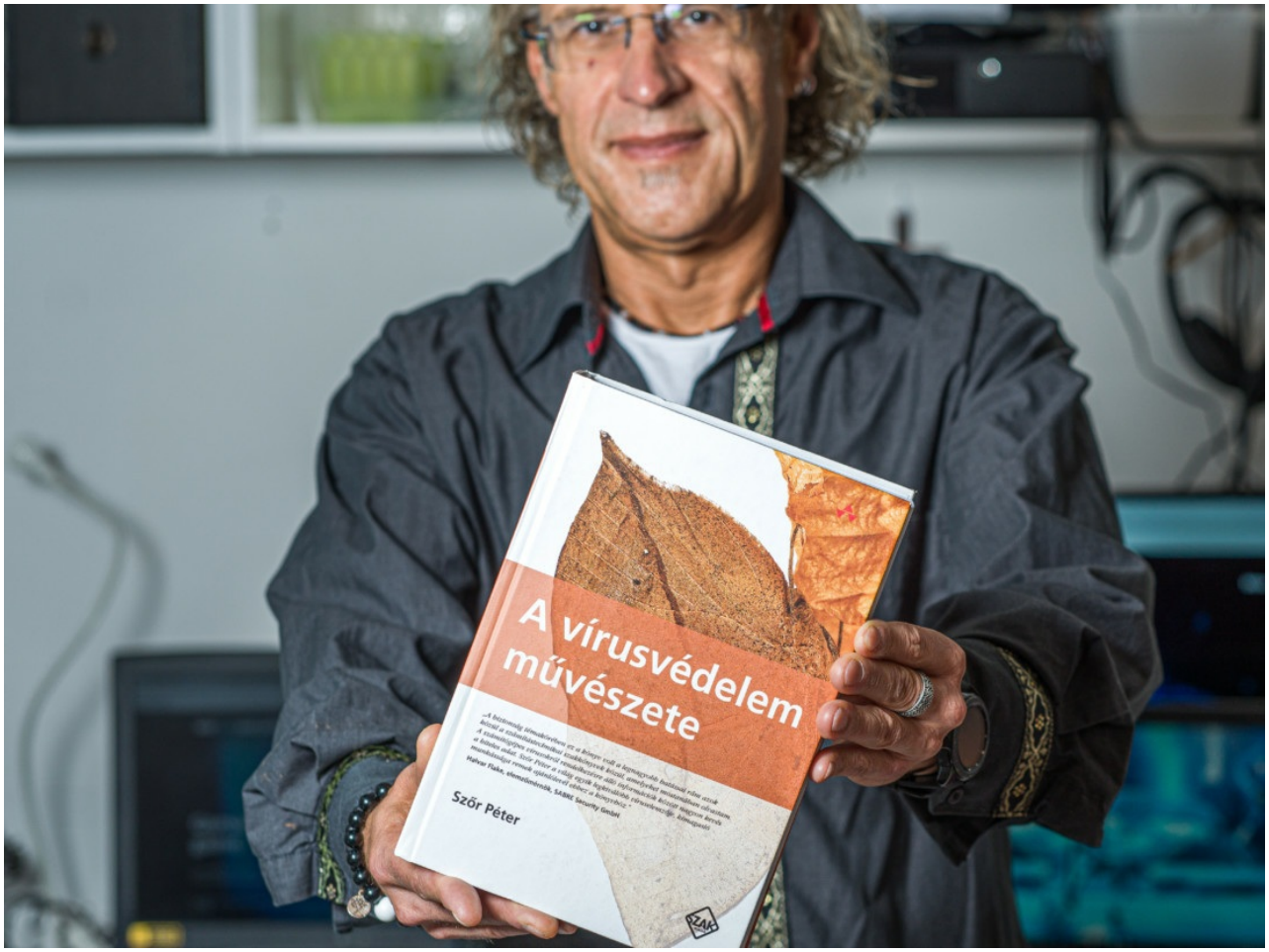
Manapság az információhoz könnyen hozzá lehet férni. Én mikor annyi idős voltam, mint te, elmehettem a Szabó Ervin könyvtárba, és ha ott valamit nem találtam, az egyetemi könyvtárba a Felszabadulás-térre. Ha ott sem volt meg, nem tudtam mit kezdeni. Te ma leülsz a Google elé, ott a Wikipédia és hasonlók, pár perc alatt megvan bármi. Ez nekem nagyon tetszik.

Na igen, de ezzel vissza is lehet élni. Te is említetted a Facebookon bármit megosztó embereket, de vannak ennél furcsább helyzetek is.

Ez egy mellékhatása a dolognak, ami egyre fontosabbá válik. Kezdetben volt a Photoshop, aztán jött a deep fake, ebből meg tavaly augusztusban a Samsung laborja elkészített egy algoritmust, ami egyetlen darab állóképből deep fake videót tudott csinálni. Meg is csinálták a beszélő Einstein és Mona Lisa videókat. Ezek alapján a fake news egy élő problémává vált, és nem csak választások vagy krízishelyzetek esetén, hanem tulajdonképpen mindig. De vannak fogódzók ebben is. Fontos, hogy a diákokat is tanítsuk a biztonságos internetezésre. Én 2013 óta tartok iskolai órákat.

Ezt, mint Sicontact Kft.?

Kezdetben még a Safer Internet berkeiben, aztán most már a Sicontact Kft. szakértői csapatának tagjaként. Szerencsére partnerünk, az ESET számára is fontos, hogy a gyerekekhez, szülőkhöz is eljuttassuk azt a tudást, amiről azt gondoljuk, hogy segítheti őket a tudatos számítógép használatban. Sokféle témát feldolgoztunk már együtt, például érdemes megtanítani nekik, hogy mit higgyenek el, mi a fake news és hasonlók.



Szőr Péter a magyar informatika és víruskutatás meghatározó alakja volt, 2013-ban hunyt el, tiszteletére szakmai díjat alapítottak (ez a Virus Bulletin által odaítélt Péter Szőr Award). István szerint Szőr 2005-ös könyve máig szakmai alapmű // Fotó: Sebestyén László

Az információ hitelessége is olyan, amivel egyre többet kell foglalkozni a felnőtteknek és a gyerekeknek is. Az egyik előadás anyagomban benne van például, hogy a Wikipédián fent volt egy kitalált ország kitalált háborúja öt és fél éven keresztül. Függetlenül attól, hogy önkéntes szerkesztők ezt folyamatosan nézegetik, mégsem szúrt szemet a dolog senkinek.

> Erről eddig egyébként nem volt szó, de szeretném kiemelni, hogy nincs ma már olyan platform, amire ne kellene vírusirtó.

Régen még voltak olyan elképzelések – amiket én már akkor is vitattam –, hogy a Linux és a Macintosh eleve védett. Most pontosan utánanéztem: 2012-ben volt egy 600 ezer gépet számláló botnet, csak Macintosh-gépekből. JAVA-sebezhetőségen keresztül fertőzte meg a gépeket és zombihálózatot alkotott. A Wayback Machine mond valamit?

Persze.

Na, azon meg lehet nézni az Apple honlapját. A régi állapot azt írta: itt nincsenek vírusok. Aztán mikor egy botnet miatt kellett kibocsátaniuk egy malware-removal frissítést, gondolhatod, hogy fogcsikorgatva, de akkor már azt írták: ez egy biztonságos

platform és ők mindent megtesznek, hogy az is maradjon. Ezt a két képet egyébként egymás mellé rakva mutattam be egy előadáson. Lényeg a lényeg: rengeteg sebezhetőség van, vírusirtó mindenre kell.

Rengeteg olyan platform van, amire viszont nem tudsz ilyet telepíteni. Eszembe jutnak az okostelevíziók, amikről szintén rengeteg helyen lehet olvasni, hogy nem biztonságosak.

Látnod kellene a fertőzött okostévéket, amiket a zsarolóvírus lezárolt!

Oké, de akkor mit tehet a felhasználó? Mit tehetek én, aki mindent frissítek, mindenhová letöltöm a megfelelő vírusirtót, de például a Playstationre nem tudok ilyesmit telepíteni?

Ritka azért, hogy efféle támadás történjen. Sokféle hiányossága van egyébként a biztonsági szakmámnak. Az okosóráktól kezdve az egészségügyi eszközökön át az IoT-termékekig. Elképesztő! Volt egyszer egy előadás, ami ezekről az eszközökről szólt.

> Az inzulinpumpát és a szívritmusszabályozót is meg lehetett hackelni. Nincs autentikáció, se jelszó, nincs titkosítás, meg rendszeres frissítés.

Az inzulinpumpával például meg lehetett csinálni, hogy ugyanazon a wifin clear textben „hallgattad le" az adatokat, majd újra és újra beadtad az inzulint. Ezzel meg tudod ölni a másik embert. És ezek orvosi eszközök, mégis elképesztő hiányosságaik vannak. Úgy tudom, hogy 2022-re irányozta elő az Európai Unió a SecureIoT programot, ami pont ezeknek az eszközöknek a védelmét írja elő.

Ha valakinek meghackelik a pacemakerét, az egy célzott támadás. A blogodon viszont inkább olyan támadásokról írsz, amiket csak úgy kiszórnak online és bíznak a szerencsében. Van arra statisztika, hogy Magyarországon mennyire gyakori a célzott kibertámadás? Számíthat erre valaki?

Magyarországi statisztika sajnos elég ritka. A CERT-ek szoktak néha kitolni magyar statisztikákat, mi is inkább a külföldiekhez férünk hozzá. A Covid-kapcsán gyűjtöttem párat egyébként, egyet megkaptam én is személyesen. Eszerint a magyar kormány és a WHO jóvátételt ajánl fel, 80 vagy 100 ezer forintot. Kérik szépen, hogy minden személyes adatunkat adjuk meg, ideértve a bankkártya-adatokat is.

Te is kapsz vírusokat?

Hát, a spam-folderbe jönnek ilyen próbálkozások. Ezeket rendszeresen meg szoktam nézni, és van olyan, hogy tollhegyre tűzöm, foglalkozom velük. Régen a Török Szultán, meg a Fülig Jimmy fogalmazta meg a leveleket Google-fordítóval, ez most viszont egész tisztességesen meg volt írva. Persze az ember fejében kigyulladhat a villanykörte, hogy

mégis miért kellene a magyar kormánynak ennyi adatunk. De ez is mutatja a fejlődést. A bűnbandáknak akár magyar tagjai is lehetnek, vagy a szolgáltatásként bérelhető botnet-csomagoknak lehet a része a fordítás.

Ez hogy néz ki a gyakorlatban? Felmegyek a dark webre és veszek egy kibertámadást?

Igen, malware-as-a-service-ként lehet igénybe venni. Adnak hozzá 24 órás supportot, kiválaszthatod, melyik bank ügyfelei ellen akarsz támadást, lesz, aki folyamatosan segít neked.

Sok helyen írták, hogy a koronavírus-járvány miatt megemelkedett a támadások száma.

A Gmail áprilisban írta, hogy hetente 126 millió Coviddal kapcsolatos adathalász levelet blokkoltak és észleltek. A Barracuda azt írta, hogy márciusban 600 százalékos emelkedést tapasztaltak az adathalász támadásoknál. Az FBI meg kiadott egy felhívást, ami a kriptovalutás csalásokra hívta fel a figyelmet. Volt ezek között nagyon jó kamattal kecsegtető befektetés, illetve jótékonysági szervezeteknek való adakozás, ami nem valós adatokra épült. Olyan ez, mint mikor olimpiát rendeznek, eltűnik egy maláj repülőgép, vagy valami hasonló világesemény van. A bűnözőknek mindegy, hogy háború van vagy természeti csapás –

> ők mindegyikre kitalálnak egy kedvező levelet, ami szerint Bill Gates rád hagyományozza a vagyonát, ha e-mailt írsz neki. Ki ne akarna ingyen kapni 100 ezer forintot?

A koronavírus-járvány ilyen szempontból nagyobb dobás volt, mint mondjuk az általad is említett olimpia?

Nem tudom megítélni, de ez is egy jó alkalom volt arra, hogy több különböző területen próbálkozzanak. A zsarolóvírusokról talán nem kell beszélni, mindenki látott olyan embert, aki látott olyan embert, aki látott zsarolóvírust. Ezen túl egy csomó túlárazott, nem is létező védőeszköz került fel az online piacterekre, amikre akár a rendőrség is lecsapott. A Jófogáson én is láttam a saját szememmel 15 ezerért ezerforintos maszkot. A briteknél már az első hónapban, márciusban 800 ezer font kárt okoztak a maszkokkal kapcsolatos csalások – ez mintegy 300 millió forint.

A home office hogy befolyásolta ezt?

Ez ott kavar be, hogy mindenki otthon dekkol, temérdek szabadidővel – kis túlzással, mert ha a gyereknek kell a házi feladatban segíteni, az elvisz rengeteg időt. *(Nevet.)* Csakhogy mindenki hazamenekült a gépével, ami elég vegyes képet mutat. Ahol nem készültek fel rá és csak egy gép van, ott azon tanul a gyerek és minden felnőtt is ahhoz fér hozzá. Ez alapvetően nem így kéne működjön, hanem egy dedikált gépen kéne dolgozni, egy másikon meg hülyeségeket nézegetni, tiktokozni.

Aztán az kéne, hogy biztonságos legyen a beléptetés, VPN-nel lépj a céges hálózatba – ahol ezt nem tudták megvalósítani, ott ez nagyobb kitettséget okozott. Azon túlmenően, hogy eddig az emberek a munkájuknak egy részét végezték számítógépen. Most mindenki számítógépen végezte az összes munkafolyamatot. Az, hogy ezt hipp-hopp, gyorsan kellett megvalósítani, azokon a helyeken, ahol nem tartanak rendszeres biztonságtudatossági képzést, ahol a policyk elkészítése és betartatása elmarad, okozhatott ez sok nehézséget.

És itt visszautalnék a beszélgetés elejére, ahol szó volt róla, hogy a kkv-k nehéz helyzetben vannak. Ahol egy pár fős csapat van és nincs biztonságtechnikai szakértő, ott még ha kértek segítséget valahonnan is ők lettek a legkevésbé felkészültek.

Lesz ennek hosszabb lefolyása? Ezek a cégek számíthatnak fél-egy éven át tapasztalható kellemetlenségekre?

Nem vagyok jós, nem tudom ezt megjósolni. Az biztos, hogy nagyon sok adatlopás van, és ezek nem mindig derülnek ki azonnal. Van ugye e a HaveIbeenpwned nevű weboldal, ahol már nem is tudom, hány milliárd ellopott jelszónál tartanak.

De a már említett zsarolóvírusok egyre kellemetlenebbek, és vannak köztük olyanok, amik kifejezetten céges adatokra utaznak. Átfésülik a hálózatot és ahol vállalati adatokat találnak, ott minél nagyobb kárt próbálnak okozni. A titkosítás is villámgyorsan lefut, másrészt elég az első pár ezer bájtot elkódolni, onnantól már az állomány használhatatlan lesz. És el is lopják a fájlokat. A zsarolás kiegészül azzal, hogy nemcsak elveszted az adataidat, hanem ki is teszik őket egy publikus weboldalra. Egy cég sok kényes, bizalmas adatot kezel. Ennek a kockázata mindig megvan és ha nem veszed észre, hogy veled ilyen történt, akkor később is bajba kerülhetsz.

Tegyük fel, hogy egyik nap bekapcsolom a gépem és felugrik a böngészőben, hogy ennyi és ennyi adatod van nálunk fizess 100 ezer eurót, vagy mindened oda! Mit tehetek?

Attól függ. A saját gépedről beszélünk, vagy a munkahelyi gépedről?

Ez is jó kérdés, mert sok ember nem tudja, hogy ezeket külön kell kezelni.

Pedig illik. Ha munkahelyi, akkor a főnökkel és a rendszergazdával kell egyeztetni.

A zsarolóvírus egyébként nálam nagy mérföldkő volt. Én olyan korban nőttem fel, amikor még nem volt személyi számítógép. Bicikliztem, fociztam, kirándultam. Aztán jött a számítógép, amit én nagyon szeretek és minden nap próbálok tanulni róla valami újat.

> Eleinte a vírusok sem voltak kimondottan gonoszak. Eljátszották a Yankee Doodle-t öt órakor, hogy lejárt a műszak, menj haza. Fejre állították a képernyőt, vagy leestek a karakterek az alsó sorba, de ha újraindítottad a gépet, tudtál tovább dolgozni.

Később megjelentek azok, amik töröltek fájlokat vagy folyton újraindították a géped. Most viszont ez kifejezetten olyan káresemény, hogy saját fájljaid tűnnek el. A diplomamunkád, családi fotóid és hasonlók. A sarki boltban tudsz másik Windowst venni. A személyes dolgaidat nem tudod visszaszerezni. Egyébként sok esetben még ha fizetsz a zsarolóknak sem mindig kapod vissza őket.

> Nem Grál lovagokkal, hanem bűnözőkkel üzletelsz.

Ráadásul ezzel csak bátorítod a kínai vagy szentpétervári állástalan programozót, aki rögtön szól a haverjának, hogy hé, írjunk még több ilyen kódot, mert működik a modell.

Tehát mit tehetek?

Naprakész vírusirtót használsz. Folyamatosan frissíted az operációs rendszered és az alkalmazói programjaidat. És rendszeres mentéseket végzel. Ezek mehetnek felhőbe vagy külső tárhelyre. Olyanra, ami csak a mentés idejére van csatlakoztatva. Ezen felül légy biztonságtudatos. Hiába teszem meg ezt a három lépést, ha jön egy warez program, ami azt mondja, hogy ő majd futtatja nekem a kalózverziós játékaimat, csak annyi a dolgom, hogy előbb kikapcsoljam a vírusirtót, ami védene. Ha nincs a helyén az eszed és te vagy a gyenge pont, akkor el tudsz vérezni ezen. Cégeknél jön még ehhez, hogy jól kell bekonfigurálni mindent, ne legyenek nyitott portok. A supportos srácok nálunk azt mondják, hogy a ransomware fertőzések 60-70 százaléka a nyitott távoli asztalelérés RDP protokollján keresztül jut be.

A blogodat is a tudatosságra való nevelés okán kezdted írni 2007-ben?

Igen. Ez volt az első blogom, nagyon féltem, hogy mi lesz, ha lélekromboló kommentek jelennek meg. Persze van egy egészséges önbecsülésem is. Azt fájlalom, hogy az ember szeretne ismeretet terjeszteni, széles körhöz eljuttatni ezeket az információkat. Ha találkozom szakmabeliekkel, mindig dicsérnek, hogy milyen jó a blog. Ebből látszik, hogy az az állandó pár száz fő, aki ezt szokta nézni, na, ennek a felét ők teszik ki. Pedig ők már nem tanulnak belőle semmit, hiszen tudják ezt, csak csekkolják, mint kollégát. Amikor viszont valami kikerül az Index címlapjára, akkor tud 4-5-6-8 ezerre felmenni. Az OTP-s poszt, ami ma került fel a címlapra, az 50 milliós csalásról, az nagyon jól ment.

Erről pont akartalak kérdezni. Nem ez az első ilyen csalás, amiről idén hallunk, volt már szó egy eset 30 millió forintról is. Ez most elég forró téma.

500 millió Facebook-felhasználó adatai vannak a dark weben, állítólag 370 ezer magyar adatait is árulják. Egy csomó ellopott jelszó is van emellett. Mikor ellopják a személyes adataid, sokan mondják, hogy hát ők nem Trump elnök, nem érnek semmit az adataik, kenjék a hajukra a hackerek. Holott sokkal jobb, ha ellopják a pénzedet, mert az csak pénz, mintha ellopják az útleveled, aztán tíz év múlva letartóztatnak az olasz határon.

Az első esetben is hasonló volt a probléma gyökere. Korábban is ellophatták már a személyes adataik egy részét, most viszont ellopták az aláírási címpéldányt és megpróbálták megszemélyesíteni a károsultakat. A bankok szigorúak, a mobilszolgáltatók ugyanakkor viszonylag könnyen hajlamosak átírni személyes információkat. Én is csak azt tudom, amit a cikkek írtak, de úgy tűnik, SIM-kártya cserés csalásról volt szó, azaz a banki biztonsági SMS-t térítették el. Erről a már említett posztban részletesen írtam.

Érdekes, hogy ezt mondod, mert én is hallottam olyan cégről, ahol kivezetnék az SMS-alapú kétlépcsős azonosítást, mondván: nem annyira biztonságos, mint sokan gondolják.

Már 2014-ben megjelent egy telefonos kártevő, aminek fejlesztésében az a Marcus Hutchins is benne volt, aki később megmentette a világot a WannaCry zsarolóvírus támadásától. A ZeuS el tudta téríteni a kétlépcsős azonosítás SMS-eit és továbbította őket a bűnözőknek. A SIM swap annyiban más, hogy elnémul a telefon, amikor leválasztják a hálózatról, és ekkor egy másik készülék kezd üzemelni.

> Ebben az esetben a szolgáltató munkatársa azt mondta az ügyfélnek, hogy azért némult el a készüléke, mert a kőbányai hálózattal gond van, telefonáljon vissza később.

Na most az sem egy jó vezetői hozzáállás, hogy ha baj van, igyunk meg pár kávét, menjünk el húsvétozni, és majd utána ránézünk, hátha már megjavult. Mert a problémákat úgy szokás megoldani, hogy megnézzük, mi okozza őket. A supportosnak pedig tudnia kell, mi a SIM swap és meg kellene néznie, mi történt az adatlapon – akkor rögtön látta volna, hogy kártyacsere történt az illető nevében.

Ezek szerint nem is a kétlépcsős azonosítással van a probléma?

Én azt mondom, hogy ha mindenki igénybe venné a kétlépcsős azonosítást, már azzal is jobb lenne a világ.

Szóba jött korábban a GDPR. Erről mi a véleményed?

Emlékszel te még az ötvenes törvényre?

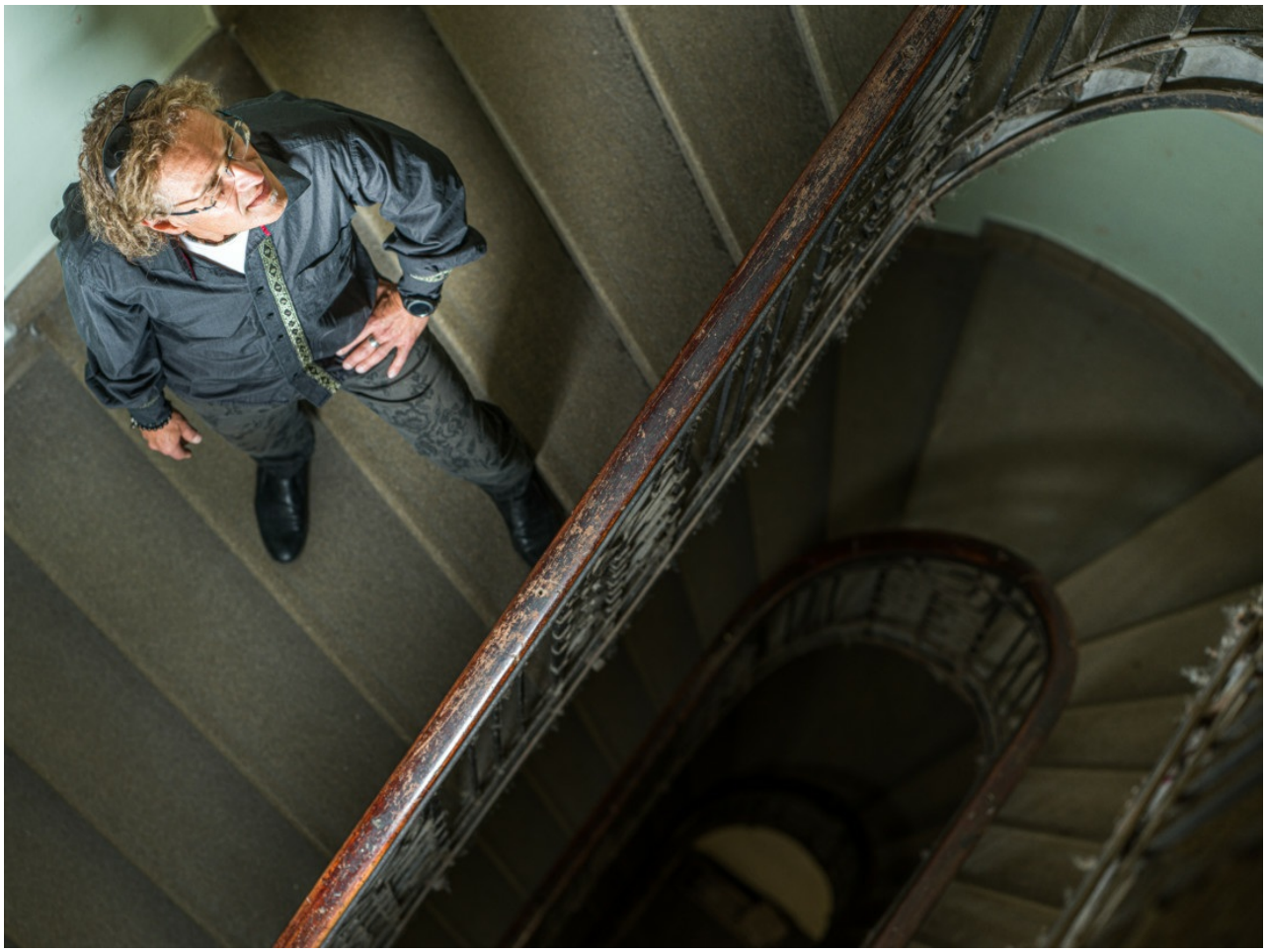
Nem.

2013-ban jelent meg, állami és önkormányzati szervezetek részére íródott L. számú adatbiztonsági törvény. Volt benne kétévenkénti felülvizsgálat is. Adatvagyon-leltárt kellett készíteni, adatvédelmi felelőst kinevezni. Még talán a mai napig sem tudja ezt minden szervezet betartani.

> Jártam olyan kórházban, ahol még XP meg Windows 95 futott azon a gépen meg ilyesmik.

Hány éve? Csak hogy megnyugodjak.

Tavaly. Voltam olyan biztosítónál is, ahol Windows 95 volt, az is tavaly. Nyilván egy ilyen törvényhez szakembert meg erőforrást kell biztosítani. De arra jó volt – és ezzel egyetértés volt a szakmában –, hogy legalább a gondolkodás homlokterébe került a probléma.



István maga is használ okosórát, kulcstartóján viszont nem sima USB-kulcs, hanem biztonsági lakat, mert sosem lehet tudni. Egy biztos: a beszélgetés után komoly jelszócserébe és frissítésbe kezdtem, biztos, ami biztos. // Fotó: Sebestyén László

Ugyanez a GDPR. Egyrészt ügyvédeket kell foglalkoztatnod, másrészt IT-biztonsági szempontból is meg kell tervezned az adatfelhasználási folyamatokat. Megint csak azt gondolom, hogy ha egyáltalán eleget lehet tenni ezeknek az előírásoknak, a magánszemélyek ebből rájöttek, hogy milyen jogaik vannak az adataik felett, és a cégek is elkezdtek ezzel foglalkozni. Ez szerintem összességében egy jó dolog.

Borítókép: Csizmazia-Darab István, a Sicontact kft. IT biztonsági szakértője // Fotók: Sebestyén László