Kovács Zsolt

Információvédelem

Az (Ön?)Tudatos Felhasználó Kézikönyve
avagy az egészséges paranoia

E dokumentumnak célja, hogy általános és figyelemfelkeltő információk fókuszba helyezésével megkíséreljen változtatni az Ön hozzáállásán azzal, hogy megkérdőjelezteti Önnel a biztonságról alkotott véleményét.

A Működésbe vetett hit - Felhasználói ismeretek

A Számítástechnika-történet kezdetén, a számítógép kizárólag olyan személyek számára volt elérhető, akik értettek hozzá. Saját gyermekük volt az eszköz, melyet kutató laboratóriumokban, egyetemeken vagy éppen katonai célú létesítményekben fejlesztettek elsősorban elvont matematikai fogalmak, számítások elvégzésének céljából.
A számítógép volt a válasz a problémára, melyet már a XVII. században Blaise Pascal is látott, amikor megalkotta az első mechanikus számológépét.

40-es évek. A születés pillanata. Az ENIAC alkotói. E lelkes, elhivatott úttörők voltak az első *Felhasználók* is, akik ismervén az *Eszköz* gyengeségeit, ki tudták kerülni annak hibáit is. A Felhasználás nem volt egyszerű, javarészt fejben fejlesztettek programokat, és akaratukat papírra lyukasztgatva tudatták a Géppel. A rendszer hibáit hagyományokon, vagy éppen az egyéni leleményességen alapuló megkerülő megoldásokkal igyekeztek közömbösíteni. E tudás volt tulajdonképpen az első Felhasználói ismeret, melyet a területen tevékenykedők egymás között igyekeztek terjeszteni. E hozzáértők egymástól abban különböztek, hogy mely hibára volt megoldás a fejükben, illetve hogy tagjai voltak-e annak a közösségnek, amely már talált megoldást az adott problémára.

Ez volt a hajnal. ***EMBER*** tanított gépet, ***EMBER*** tanított ***EMBER***t és az adta tovább a Tudást, mely az Eszköz használatát volt hivatott elősegíteni.
A 70-es évek végen, az arany 80-as évek kezdetén a háztömbnyi, de legalább két és fél ajtós szekrény méretű számítógép – hála Stephen Gary Wozniaknak és a többi úttörőnek - az egyetemek falain átlépvén mindennapos használati eszközzé vált. Ez volt a Home Computer kora. 1981-ben megjelent az IBM PC és a Home Computer, személyi számítógéppé vált!

A hardver fejlődése olcsóvá és ez által elérhetővé tette a számítógépet mindenki számára!

Természetesen ez nem történhetett volna meg a szoftver, valamint az Operációs rendszerek, fejlődése nélkül. A Szoftver fejlődésének iránya és célja az, hogy minél kevesebb ismerettel lehessen használni a személyi számítógépet.

Volt egy pont, ahol olyan ***EMBER***eknek köszönhetően mint Steve Jobs és Bill Gates - hogy csak a legismertebbeket említsem – Mi, többiek is Felhasználókká váltunk!

Ám az Operációs rendszerek fejlődése változatos mellékhatásokkal is járt. A Tudás kikerült az értő fejhasználók kezéből, olyan ***EMBER***ekhez akiknek a számítástechnika nem alaptevékenységük.

1949-ben Neumann János egy tanulmányában (*Theory and Organization of Complicated Automata*) felvetette elméletét, miszerint a számítógép programok képesek a szaporodásra. Néhány évvel később az elméletet a Bell Labs munkatársai a gyakorlatban szemlélteték a

Core Wars nevű számítógépes játékkal, de 1981-ig kellett várni az első valódi vírus megjelenéséig. Ekkor született, és szabadult el az Apple II Elk Cloner vírus. A vírus elnevezést 1983-ban Frederick Cohen találta ki, aki különös hasonlóságokat fedezett fel a biológiai és a számítógépes vírusok szaporodási formái között.

A 90-es években a boot sector vírusok voltak rendkívül divatosak. A vírusok a floppy lemezek boot sectorába fészkelték be magukat, s mivel a lemezek baráti (***EMBER***i) körben kézről kézre jártak, mindenegyes gépet megfertőztek, amelybe a lemezt beletették. Hasonló fájl-fertőző vírusok is elterjedté váltak. Ezek futtatható programokhoz, pl.: .bat .exe .com fájlokhoz kapcsolódtak.

Ezek a vírusok azonban még relatíve lassan terjedtek, mivel a floppykat fizikai úton kellett átadni és továbbítani az ***EMBER***ek között.

1995-ben jelent meg az első, széles körben elterjedt, Concept nevű makró vírus. A makro vírusok a makró fejlesztő nyelv (elsősorban a Microsoft Office makró nyelve) parancsait használták ki. Ez már elsősorban dokumentumokban, csatolmányként e-mailben terjedt, de későbbi (pl.: Melissa) társaihoz képest még jóindulatú volt.

A Morris Worm és a boot szektor vírusok a számítógép ismert gyengeségeit használták ki, vagy ***EMBER***i közreműködést igényeltek a terjedéshez.

Ma sincs ez másképp!

Malware, Phising-, Spam és Hoax

Van azonban egy pár tényező ami megváltozott az idők során. A korai időszakban a az ártalmas kódok vagy nem tettek semmit, vagy tényleges kárt okoztak. Elsősorban önnálóan üzemelő munkaállomásokat támadtak meg. Lényegesen változott a terjedés módja: az Internet-használat rohamos terjedése nyomán és a cél ma már nem elsősorban egy önnáló munkaállomás működésének akadályozása, sokkal inkább a kiterjedt hálózatok, a hálózatba kapcsolat számítógépek működésének akadályozása az által, hogy felesleges, és feleslegesen nagy forgalmat generálnak tevékenységük során a hálózaton, ezzel bénítva a szolgáltatások elérését! Lényegesen változott a cél: ma már az információ szerzés-, lopás áll első helyen e programok küldetésében.

Malware - Ha abból a szempontbó vizsgáljuk az ártalma kódokat, a vírusokat, trójai programokat (trojan), a metamorf és polimorf vírosokat, férgeket (worm), a kémprogramokat (spyware), stb. megállapíthatuk, hogy a következő két fogalom mindegyikre érvényes: programokról beszélünk és valamilyen módon kért okoznak, szemben az „igazi" programokkal, melyek a munkánkat segítik. Gyüjtőnevükön ezért ezeket a kódokat, ***malware*** (malicious software, károkozó program) nevezzük. A továbbiakban ezzel a névvel hivatozom rájuk.

A Malware magától szaporodik úgy, hogy a fertőzött gépen található címjegyzékben szereplő mindenegyes személynek tovább küldi magát, vagy a rendszerek valamilyen gyengeséget kihasználva az Internethez csatlakozók millióit támadja meg.

A *Malware* napjainkban az e-mail farvizén hajózik el a tűzfalak mellett. A MessageLab felmérése szerint minden 276-ik e-mail fertőzött.

Az újabb, több kapcsolatra épülő számítástechnikai rendszereknek és kommunikációs csatornáknak köszönhetően mára mindenkinek van e-mail hozzáférése. Rövid idő alatt többszázezer, ha nem millió host fertőződhet meg. 1999-ben a Melissa 4 nap alatt okozott sok millió dolláros kárt. A LoveBug vírusnak ehhez alig 5 óra kellett. Bár az SQL Slammer/Sapphire féreg nem e-mailen terjedt, jól jelzi mire számíthatunk: a legtöbb kárt élete első 10 percében okozta!

Mivel az e-mail segítségével gyakorlatilag valós időben terjedhetnek a vírusok, az e-mail az egyik legkiválóbb fertőzéshordozó. 1996-ban a vírusok csupán 9%-a kapcsolódott az e-

mailhez, és 71%-uk a floppy diszkek cserélgetéséhez. 2002-re a floppyk miatt nem keletkezett fertőzés, de az e-mailben érkező vírusok immár a fertőzések 86%-áért tehetők felelőssé.

HOAX *vagy lánclevél* - az ***EMBER***i jóhiszeműséget kihasználva, vagy vírus veszélyre figyelmeztet, vagy pénzkereseti lehetőséget kínál, vagy segítséget kér, vagy csak egyszerűen vicces. A rendszer kapacitását feleslegesen foglalja, az ***EMBER***ek idejét rabolja, így a cégeknek tetemes anyagi veszteséget okoz (egyesek szerint 1 dollár/hoax). A spammerek a hoaxokból gyűjtik az e-mailcímeket. Sajnos HOAX működési rejtelmei meghaladják e dokumentum tervezett terjedelmét, ám mivel ez az ismeret rendkívül fontos, nyomatékosan javaslom az alábbi oldal elolvasását!

FONTOS! Lánclevélküldők tanfolyama http://yikes.tolna.net/hoax/

A ***phising*** spam pop-up üzenetek vagy e-mail segítségével téveszti meg az egyszeri felhasználót, s csalja ki tőle hitelkártyája számát, bankszámla adatokat, TAJ számot, jelszókat, stb. A csalók üzeneteikben a felhasználó által ismert szervezetnek vagy cégnek adják ki magukat, s általában arra kérik a felhasználót, hogy számlája adatainak „frissítése" vagy jóváhagyása céljából látogasson el a cég oldalára (vagy legalábbis egy oldalra, amely tökéletesen úgy néz ki, mint a valódi szervezet vagy vállalkozás honlapja – paypal.com - ahol a kis „l"-t nagy „i"-re módosították). Itt általában banki és egyéb személyes információt kérnek a gyanútlan felhasználótól, s az űrlapok kitöltésének elmulasztásáért büntetést helyeznek kilátásba. Így megszerzett jelszavakat, banki és személyes adatokat a csalók bűncselekmények elkövetése során felhasználják fel, az ártatlan felhasználó nevében akár milliárdos károkat is okozhatnak,de legalább is megkönnyítik az áldozat bankszámláját!

Egyes statisztikák szerint az adatlopásra tett próbálkozások a felhasználók 5%-nál sikeresen végződnek!

A vállalatok többségének - annak ellenére, hogy rendszereik modernek, a védelmük erős - nap mint nap szembe kell néznie a Malware támadások következményeivel. Ennek elsődleges oka, hogy nincsenek, vagy nem tartatták be a felhasználókkal a védelmet szolgáló szabályokat!

A Malware védelemmel kapcsolatos intézkedésekről nem feltétlenül kell tudniuk a felhasználóknak, hiszen ez nem érdekli őket, de az sem megoldás, hogy minden csatolt állományt letiltunk, hiszen ez az e-mail egyik legnagyobb előnye. Meg kell találni a biztonság és a felhasználók kényelme közötti egyensúlyt!

A felhasználó: minden biztonsági rendszer leggyengébb láncszeme!

Az összetett férgek terjedésétől a makró vírusok burjánzásáig, minden egyes Malware végeredményben egyetlen dolgon alapszik: az ***EMBER***ek természetüknél fogva megbíznak egymásban, így könnyen becsaphatók. A vírus ellenőrző programok s más Malware ellenes intézkedések a biztonság hamis illúziójába ringathatnak.

Azonban tökéletes biztonság nem létezik!

A felhasználóknak tisztában kell lenniük a *social engineering* néhány alapvető módszerével!

A természetes bizalom és a social engineering

A *social engineering* az emberek természetes bizalomra való hajlamának kihasználása. Hackerek vagy akár egyszerűen rossz szándékú emberek is gyakran használják ezt a módszert a számítógépekhez való illetéktelen hozzáférésre és információk megszerzésére. A social engineering nem a hardver, a szoftver vagy a hálózat hibáit, hanem az emberi természet gyengeségeit használja ki a számítógépek feltörésére, vagy éppen az Információ megszerzésére.

A „támadás” nem feltétlenül a számítógéppel lefedhető kommunikációs csatornák felől érkezik! Ellenkezőleg! A célzott támadás felhasználja valamennyi kommunikációs csatornát, az emailtől a telefonon át! A Social engineering, Malware és phishing támadások közösek abban, hogy a megtévesztésre alapoznak.

Hatalom – Megfelelő határozottsággal fellépő személy kérésének, utasításának, érzelmi nyomásának hajlamosak vagyunk automatikusan eleget tenni, ha ezt egyéb körülmény is alátámasztja. Elég lehet a hivatkozás a nevén nevezett felettessel történt személyes megállapodásra, sürgető körülményre, határidőre, érdekmúlásra, anyagi veszteségre, az ezek miatti felelősségre vonás kilátásba helyezésére és már is nyitva áll az út az információ felé!

A támadó olyan valakinek tünteti fel magát a kommunikáció során, aki hatalommal rendelkezik. Felettesnek vagy esetleg leendő üzleti partnernek álcázza magát, adott esetben a Főnök és a cég érdekeire hivatkozva kér el olyan információt, mely információ megléte a Támadás további lépéseinél a bizalom megteremtésének eszköze lehet.

A megfelelő zsargont, hangsúlyt, hanglejtést, testbeszédet használó személy viselkedésével váltja ki a megfelelő reakciót az áldozatból. Ennek gyökerei vélhetően a társadalom hierarchikus felépítésében rejlenek. Az Emberek közötti kommunikáció erősen protokoll alapú. A megfelelő protokoll és a hierarchia ismerete lehetőséget ad további információk begyűjtésére és a támadás további lépéseinek előkészítésére.

Szeretet - Az emberek hajlamosak eleget tenni olyan emberek kérésének, akik képesek magukról kedvező, szeretetre méltó képet kialakítani másokban. Egy nagyon kedves és szimpatikus „új” kollegának mindenki a segítségére siet. Gyakorlatilag mindennapos jelenség az, hogy az új kolléga számára az ott dolgozó ideiglenesen kölcsönadja az identitását, hogy megmutassa, hogyan kell a vállalati rendszerből adatokat szerezni a munka elvégzéséhez.

Egy mindenki által kedvesnek ismert kolléga személyére hivatkozó, szintén kedves valakitől érkező kérés teljesítése, „a barátom barátja a barátom protokoll” alapján juttatja nyitott információs csatornához a Támadót!

Kölcsönösség – Többen szívesen teljesítenek kéréseket, ha valami értékeset kapnak cserébe. Ez az érték lehet kézzel fogható ajándék, lehet előjog, viszontszívesség vagy éppen segítség. Fokozottan így van ez, ha az ajándékot kérés nélkül előre kapják meg.

Remek példa erre az áruházi parkolóban képeslapokat és könyveket ajándékozó önkéntes, aki miután átadta ajándékát, tesz fel kérdéseket, vagy fogad el támogatást. Hangsúlyozva hogy az adomány és annak mértéke nincs összefüggésben az ajándékkal.

Természetesen nehéz ellenállni valaki olyan kérésének, aki előzőleg önzetlenül ajándékozott meg – akár a segítségével. Mitöbb ilyen esetben az ember hajlamos kihagyni a biztonsági ellenőrzéseket, lévén minél hamarabb túl szeretne lenni a viszontszívességen, hogy figyelmét az ajándéknak szentelhesse, vagy egyszerűen visszatérjen munkájához.

Következetesség – A vállalati biztonsági szabályok betartása mindenki számára kötelező. Mindenki tudja, hogy ez rajta számon kérhető. A számon kérő „ellenőr” személye automatikusan „megbízható”, mert Ő ellenőrzi a szabályok megtartását. Triviális, hogy ismer minden szabályt, és vele szemben a feltétlen együttműködés magától értetődően kötelező.

Gondoljunk arra az érzelmi szituációra (protokoll), amikor a Rendőr igazoltat minket! Kiváltképpen ha ez külföldön történik – szinte soha nem kérdőjelezzük meg az Ő személyazonosságát vagy az intézkedés jogosságát.

A Támadó felhívja a figyelmét az alkalmazottnak a vállalati szabályok betartására – jól ismervén a protokollt, könnyen teremthet olyan szituációt, amikor kiigazítást tesz, vagy ellenőrzésképpen kér adatokat. Az ellenőrzés végén utasítja az alkalmazottat, hogy a vállalati jelszóbiztonsági ellenőrző oldalon ellenőrizze a jelszavát – és megad egy a rendszeren kívül elhelyezett oldal címet, ami nem más, mint egy erre a célra preparált *phising landingpage*.

Társadalmi megerősítés – „Amit mindenki megtesz, számomra is kötelező” – ebből az alapgondolatból indul ki ez a támadási módszer. Kombinálva az előbbi „következetesség” módszerrel, sokkal hatékonyabban alkalmazható támadást eredményez. Lényege, hogy a telefonáló úgy alapozza meg a bizalmat, hogy név és pozíció szerint hivatkozik azokra, akik a vállalatnál már együttműködtek vele hasonló szituációban. Az áldozat feltételezvén hogy a többiek együttműködése „jogossá” teszi a kérés kiszolgálását, készségesen szolgáltat adatokat.

Szűkösség – A javak egyenlőtlen elosztásának következménye, hogy szinte genetikailag kódolt a szűkös javak iránti sóvárgás. Ezt használja ki szinte minden olyan nyereményjáték, melynek fődíja egy színes-tintasugaras-állványos-plazma-mosógép vagy egy a tízezer egyedileg dedikált, színes fogpiszkálóból! A Támadó kihasználhatja a szűkös javak iránti sóvárgást kombinálva a *lustasággal*, és a *komfort* iránti vággyal. Gondolok itt arra, hogy sok Felhasználó használ más-más rendszerhez azonos felhasználónevet és jelszót, annak érdekében, hogy Ő maga könnyen ki tudja találni. A támadónak nincs más dolga, mint ajándékot, nyereményt felkínálni egy regisztráció ellenében. Nagy a valószínűsége, hogy a regisztráció során a Felhasználó a fentieknek megfelelően kiadja a felhasználónevet és jelszót!

Képzelje el az alábbi e-mail hatását az Ön cégénél!

> From: pr@híresproduceriroda.hu
>
> To: mindenkinek@sajátcégem.hu
>
> Subject: 10 darab ingyenjegy az új Queen koncertre
>
> Tisztelt Cég,
>
> Kedves Kollegák!
>
> Minden bizonnyal értesültek a hírről, hogy az új Queen együttes ellátogat Európa több nagyvárosába, közöttük Budapestre is. A napilapokban és a szórólapokban, reklámspotokban erőssen hagsúlyozzuk, hogy az Önök cége az esemény egyik fontos támogatója!
>
> Nagylelkű támogatásukat azzal szeretnénk megköszönni, hogy a támogató cégek munkatársai között kisorsolunk 10 db darab, VIP – Stagepass-t, ami lehetőséget biztosít, hogy a szerencsés kiválasztottak testközelből élvezzék a sztárok társaságát.
>
> Amennyiben Ön is szeretne a kiválasztottak között lenni, kérjük keresse fel regisztrációs oldalunkat, és vegyen részt a sorsoláson!
>
> Fontos! A regisztrációs lehetőség kizárólag a támogató cégek dolgozóinak áll fenn! Ezért kérjük, hogy a munkahelyi címével és azonosítójával igazolja jogosultságát a sorsoláson való részvételhez!
>
> A regisztráció a http://10.104.55.63/queen/budapest/viponly.php oldalon érhető el!
>
> Üdvözlettel,
>
> A szervezők!

Ön regisztrálna? Ismer Ön valakit, aki biztosan? Elképzelhetőnek tarja, hogy ugyanazt a jelszót fogja használni, amivel egyébként a levelezése is elérhető? Lehet, hogy a levelezési jelszó hozzáférést biztosít a fájlszervereken lévő információkhoz? Talán az intranet rendszerhez is?

Rutin – A legtöbb támadásnak a recepció, az ügyfélszolgálat van kitéve. Ha a támadó történetesen ismeri a szokásos ellenőrző módszereket, némi háttér-információval felfegyverkezve kihasználhatja a rutin jellegű munkavégzésből adódó biztonsági réseket. A monoton munka óvatlanná teszi az embert. Vizsgáljuk meg ezt közelebbről. Ha Ön egy gyorsétteremben olyan termékeket rendel, melyek megtalálhatóak a választékban, úgy az

eladó rutinszerűen kiszolgálja kérését, míg ha a termék valamely tulajdonságára utal a neve helyett, a folyamat megszakad és kérdéseket fognak feltenni. A dolog pontosan így működik, aki rendelkezik minden olyan adattal mely a pontos kiszolgáláshoz szükséges, fel sem merül, hogy nem jogosult a kiszolgálásra. Sőt miután így „igazolta" magát, még kérdezhet is. Ugyan kinek tűnne fel egy ügyfélszolgálaton, ha az ügyfélkódom és a pinkódom megadása után, mintegy ellenőrzésképpen rákérdeznék valamely személyes adatomra?

Figyelmetlenség, türelmetlenség – A fentiek következményeképpen egy kellően kiégett, a rutinban megfáradt alkalmazottat a munkaidő végeztének pillanatában hívva fel, meg lehet tőle tudni, hogy pontosan milyen információkat kell megadni ahhoz, hogy a kérést kiszolgálja. Tudván hogy az adott ügyfél nem rendelkezik a megfelelő jogosultságokkal – felkészületlen volt – rutinszerűen megnevezi azokat az információkat melyek a sikeres azonosításhoz kellenek – annak érdekében, hogy minél előbb tagadhassa meg a kiszolgálást és menjen haza.

A fenti felsorolás mindössze rövid bemutatása volt a **biztonság emberi tényezőjének** irányításának. Belátható, hogy a szoftveres (vírus, spyware, malware) a logikai (phising) és a protokoll alapú social engineering támadások célzott és együttes használata úgy biztosít illetéktelen hozzáférést adatokhoz, hogy közben nem érinti a hálózatbiztonsági rendszer egyetlen elemét sem. Sőt, e rendszerek szempontjából nézve, nem történik más mint az, ami minden nap minden percében történik - egy jogosult felhasználó használta jososultságait adathozzáférés céljából. Hétköznapi üzemmenet!

A *social engineering* támadások egyik legnagyobb veszélye, hogy a támadás nehezen vehető észre és mivel az információ nem vész el, így a hiánya sem tűnik fel!
Az ami nem hiányzik, azt biztosan nem lopták el! Biztos Ön ebben?

Védekezés – az (Ön)tudatos felhasználó kézikönyve

E fejezet célja, hogy a fentiek ismeretében lista szerűen felsorolja azokat a Felhasználói tevékenységeket, melyek tudatos használata erősíti a vállalati védelmi rendszer hatékonyságát, védi az információt és végső soron biztosítja a folyamatos munkavégzést a számítógéppel az információval kapcsolatos munkánk során.

A social engineering támadások elleni védekezés

Általánosan használható gyakolat nincs, nem is kell hogy legyen. A lényeg röviden összefoglalható azzal, hogy minden információt ami a képernyőn megjelenik, olvasson el, értsen meg, döntsön és csak ezak után cselekedjen. A rutin, a figyelem hiánya maga a rés az emberi bitonsági rendszeren!

- Soha ne engedje át az identitását másnak. Ne adja „kölcsön" a jogosultságait!
- A titkos jelszó, titkos!
- Új kollegának segíteni fontos, azonban győződjön meg akkor, hogy valóban az aki.
    - Hívjuk vissza a vállalati melléken!
    - Kérjük a vezetőjének a jóváhagyását.
    - Ha ez lehetséges kérjük a saját vezetőnk véleményét.
    - Ahelyett, hogy segítenénk neki az információ kinyerésében, bíztassuk a megfelelő jogosultságok megszerzésére.
- Soha ne adjon ki olyan információt másnak, amivel jogosultságai lévén önmagának is tisztában kell lennie!
- Soha ne adja ki másnak az Ő saját adatait, ha valaki, hát Ő biztosan tisztában van vele! A közérdekű információ azért közérdekű, mert mindenki eléri. Ennek ismerete nem számít tudásnak.
- Az, hogy valaki ismeri a zsargont, még nem jelenti azt, hogy megbízható.

- Mindig gondolkozzunk a SAJÁT FEJÜNKKEL, mások véleménye és magatartása irreleváns ha mi magunk (is) megtartjuk a szabályokat!
- Legyen következetes, és küldjön el e sorok írójának 5 euro-t!
- Ismerje meg saját céges folyamatait, a szabályait, de ne alkalmazza őket vakon!
- Tanuljon meg visszautasítani! – ez a legnehezebb erőpróba, ám véleményem szerint megéri a fáradságot! Használata az élet bármely területén hasznos lehet!
- Csak azokban bízzon meg, akiket SZEMÉLYESEN ismer és bennük sem vakon!
- Ne adjon át olyan információt senkinek, amelynek a forrásáról Ön személyesen nem bizonyosodott meg, hogy eredeti.
- Ne továbbítson információt harmadik személyhez az információ forrásának beleegyezése nélkül. Ha a belegyezés megszerzése nem lehetséges, továbbítsa az információ kérőjét az információ forrásához, de az információt magát ne szolgáltassa ki.
- A belső telefonszám: BELSŐ telefonszám, tehát nem publikus.
- Az hogy valaki bajban van, siet, nem lehet ok az ellenőrzés kihagyására!
- Ha valaki érzelmileg kívánja Önt befolyásolni, részrehajlásra bírni, mondjon nemet! A Szabályok alkalmazásáért még nem bocsátottak el senkit, ha igen az nem Önnek való munkahely!
- Ön EMBER és bár munkát végez, semmi nem gátolja Önt abban, hogy gondolkozzon és saját akarattal rendelkezzen olyan dolgokban, melyek az Ön felelősségei!

A Malware elleni védekezés

A modern Malware (is) az ***EMBER***ek természetes naivságát használja ki, amikor a felhasználót arra bírja rá, hogy egy hétköznapi mozdulattal segítse terjedését.

Néhány e-mail, amely jól magyarázza, miért estek sokan kísértésbe, hogy megnyissák a csatolt fájlt.

- Anna Kournikova Féreg
  Email tárgya: Tessék, itt van ;o)
  Üzenet: Szia! Ezt nézd meg!
- Melissa Virus
  Email tárgya: Fontos üzenet küldő neve-től
  Üzenet: Itt küldöm azt a doksit, amit kértél... másnak ne mutasd meg ;–)
- MyLife féreg (vagy Bill Clinton féreg)
  Email tárgya: Clinton karikatúra
  Üzenet: Hellooo! Hogy vagy? Nézd meg ezt a Clinton karikatúrát! Naaaggyon vicccess! :) :) Ígérem, tetszeni fog? Ok. Ciao.
  ==========No Virus Found==========
  MCAFEE.COM

Ezeket a támadásokat azonban vissza lehet verni a technika, a szabályok és a felhasználók megfelelő felkészítésének segítségével. A Technikai rendszerek, mint tűzfalak (csomagszűrő, statefull vagy alkalmazás szintű), Anti-vírus szoftverek, anti-spyware, anti-worm filterek működéséről és felépítéséről számtalan kiváló tanulmány, előadás és könyv született. Anélkül, hogy fókuszálnánk a fenti alapvető fontosságú rendszerek működésére, melyek AKADÁLYOZZÁK a Malware terjedését, nézzük át mely tényezők segítik azt!

A Malware terjedését rengeteg tényező segíti elő, például:

- Az Internet nyílt hálózat, így a támadások rendkívül messzire elérhetnek.
- Az informatikai rendszerek egyre bonyolultabbá válnak olyannyira, hogy sok fejlesztő nem látja át teljesen az alkalmazások működését.

- A TCP/IP-t, és a kommunikációs protokollok többségét **működőre tervezték** és nem biztonságosra!
- A szoftvereket általában nem tervezik biztonságosra.
- Egyre bonyolultabb módszerekkel védekezik a Malware az ellen, hogy elkapják.
- Az ***EMBER***ek természetüknél fogva bíznak egymásban

A fenti tényezők, és a következő gyengeségek sokasága együttesen halálos fenyegetést jelentenek a biztonságos e-mail használat számára.

- Egyre elterjedtebbé válnak a könnyen megfertőzhető multimédiás Multipurpose Internet Mail kiterjesztések (MIME)
- Az e-mail felhasználók HTML-rendering motorjai lehetővé teszik a rosszindulatú kódok és programok egyszerű végrehajtását.
- A legújabb Malware több operációs rendszert is megfertőzhet (pl.: Windowst és Linuxot egyszerre)
- Ugyanazon a gépen futó több szolgáltatás (e-mail, Web keresők, Web szerverek) egyszerre megfertőződhet.
- A polimorf Malware több fajta kódot használva megváltozik, és valós időben hoz létre új, rosszindulatú kódot, így szinte lehetetlen tovább terjedését megakadályozni.
- A metamorf Malware terjedése során más-más viselkedési formát vehet fel, így semlegesítése még a fejlettebb viselkedés-alapú vírusirtókkal is szinte lehetetlen.
- A malware-t (kiváltképp a férgeket) még útra indításuk előtt beprogramozzák az egyes rendszerek gyengeségeinek kihasználására, ezért a fertőzés sebessége hatványozva nő.
- A Malware payload-ja (kódmérete) egyre kisebb, és egyre hatékonyabb.

Egyéb e-maillel terjedő Malware: logikai bombák, billentyű figyelő (Keyboard logger), Hálózat analizátor (Network analyzers), jelszótörő (password crackers), rootkits, kém programok (Spyware). Bár nem malware, de fel lehet használni az alábbi technológiákat malware készítésére (is) : ActiveX kontrolok, Java appletek, JavaScipt, VBScript.

A P2P (fájlcserélő rendszer) terjedése révén további biztonsági tényezőket kell figyelembe venni:

- A P2P révén újabb belépési pont nyílik a céges hálózatok felé.
- Újabb hibaforrás, ahány rendszer annyi rés.
- Olyan sebezhető pont, amelyet jelenlegi vírusirtó és más Malware ellenes szoftverek sem védenek – egyelőre.
- Biztonsággal kapcsolatos felelősség számottevő része a végfelhasználóhoz kerül.
- Remek teret nyújt szétosztott szolgáltatás-megtagadás támadásra (DDoS)
- Irtózatos fenyegetés, hiszen egy időben ezernyi gépet irányíthat a rosszindulatú támadó.
- Néhány trójai program P2P programnak álcázza magát.
- Számítógép/hálózat/e-mail konfigurációról gyűjthet információt a távoli rosszindulatú felhasználó.
- A rosszul megírt P2P programok újabb biztonsági réseket ütnek a rendszeren, vagy összeomlaszthatnak gépeket.

- Néhány legális P2P szoftver a felhasználó belépésekor automatikusan frissíti a szoftverét. Ez a kényelmi funkció káros is lehet, amennyiben a frissítéseket nem tesztelték.
- P2P nagymértékben sávszélességet és tárhelyet foglalhat, így DoS támadásokat generálhat.
- A személyazonosság megállapítása nem feltétlenül biztonságos.
- Ami a mi szempontunkból elsődlegesen fontos, nem szabályozható, hogy mi megy ki a hálózatból.

A Malware járványok megakadályozása:

A felhasználók szabadon szeretnének e-mailt küldeni és fogadni, így általában az IT szak***EMBER***eken múlik, hogy a biztonság és a kényelem között megtalálják az egyensúlyt. Képtelenség mindenegyes biztonsági rést befoltozni, de a szoftveres védelem, a felhasználók oktatása, és bizonyos szabályok betartatása, valamint a szerver és a perifériák védelme nagymértékben csökkentheti a fertőzéseket és a járványok kitörését.

A kliensek Malware elleni védelme:

- Hetente futasson teljes vírus ellenőrzést, és használjon a valós idejű ellenőrzést.
- Minden fájlt, és nem csak a futtatható állományokat, ellenőriztesse!
- Heurisztikus védelem, amely a viselkedést ellenőrzi, s bizonyos parancsok végrehajtását blokkolja.
- Az aláírt ActiveX nem feltétlenül biztonságos: csak azt mutatja, honnan érkezett a kód, de azt nem, hogy mit csinál.
- A hívatlan csatolt fájlokat szabad megnyitni. Törlendőek!
- A normal.dot alap Word template legyen csak olvasható.
- A Microsoft Office alkalmazásokban a *macro security* legyen bekapcsolva, ha lehet a dokumentumokat Word 2.0 formátumban mentse el! (Ez a verzió még nem tudott makrót tárolni!)
- Az e-mail szűrő legyen bekapcsolva.
- Készítsen rendszerindító diszket, boot CD-t, boot DVD-t.
- A fertőzetlen fájlokról készítsen backupot, ugyancsak backupolja az operációs rendszer fájljait.
- Mindig látszódjék a fájlok kiterjesztése.
- A Microsoft Outlook Express betekintő funkcióját kapcsolja ki.
  (Soha ne hajoljon ki (tekintsen ki) kicsi-puha gyorsvonat ablakán!)
- Amikor csak mód van rá, ne használjon adminisztrátor vagy root jogosultságokat.
- Kapcsolja ki a Windows Script Host-ot!

Felesleges azonban olyan szabályokat hozni, mint pl.: a HTML kikapcsolása az e-mail alkalmazásokban, vagy arra kényszeríteni a felhasználókat, hogy .doc helyett .rtf és .xls helyett .csv formátumot használjanak.

Mire kell figyelni az e-mail megnyitásakor?

- Először is, még a levél megnyitása előtt ellenőrizzük, kitől érkezett levél. Ilyenkor a levelek felét azonnal törölhetjük, ha a küldő ismeretlen. – Gondolkozzon!

- Nézzük meg az üzenet tárgyát, s gondolkozzunk el azon, vajon a feladó küldene nekem olyan e-mailt, amelynek tárgya „ILOVEYOU”? Így újabb számos e-mailtől megszabadulhatunk. – Gondolkozzon!
- Ha a levél tárgyából és a feladóból arra következtetünk, hogy ez fontos üzenet, célszerű egy „zászlóval” megjelölni későbbi olvasás végett. Ezzel időt spórolhatunk meg egy feladat elvégzése és a folyamatos email ellenőrizgetés között.
- Ellenőrizzük, milyen csatolt állományok tartoznak az üzenethez. Általában a csatolt fájlok képek (jpg, gif, tiff,bmp, stb.) vagy szöveges dokumentumok (doc, wpd, wps, stb.) vagy pdf fájlok. Ha nem ismerjük fel a csatolt állomány kiterjesztését: ne nyissuk meg. E szabály betartása sokakat megkímélt volna az ILOVEYOU vírustól. – Gondolkozzon!
- E-mailben ne küldjön személyes információt!
- Törekedjen a digitális aláírás használatára! Bíztasson másokat is arra, hogy Ők is használják!
- Használjon MÁS TIPUSÚ vírusirtó szoftvert a saját gépén, mint ami a szerveren, vagy a Szolgáltatónál fut és nem lehet kérdés, hogy frissítse is azt!
- Ha az e-mailhez nem tartozik csatolt fájl, de az üzenet valamilyen weboldalra küld, szintén fontos az óvatosság. A weboldalon elképzelhető, hogy valamilyen rosszindulatú kód várakozik Önre. Ha a vírusellenőrző programunk és a tűzfalunk jól működik, általában nincs mitől tartanunk, de mi történik, ha rés van biztonsági rendszerünkben? – Nem kell minden információt magunkba tömni! A Kíváncsiság alapvető, de nem a legfontosabb emberi tulajdonság!
- Végül használjuk a józan eszünket. Ha általunk jól ismert Emberektől, cégektől (pl.: bankok) kapunk üzenetet, amely nem tartalmaz sem gyanús csatolt fájlt, sem gyanús weboldal címet, alaposan olvassuk el az üzenetet. Kis logikával látható, hogy amennyiben a bankunk írt nekünk, nem valószínű, hogy a bankszámlaszámunk megadását kéri tőlünk. Ha kétségeink lennének, telefonáljunk, mielőtt birkaként az e-mail utasításait követnénk.

Szerver és Perimeter védelem

- Legyen rendszerindítólemeze!
- Keressen olyan alkalmazásokat, amelyek közvetlenül a szerver e-mail szoftveréhez csatlakoznak - vagy vegye igénybe a Szolgáltató Antivírus szolgáltatását!
- Ha nem ismer ilyen Szolgáltatót, a dokumentum végén megtalálja azt!
    - A szerverre beérkező és onnan kimenő üzeneteket is szkennelje!
    - Ellenőrizze minden e-mail szövegtörzsét olyan kódokat keresve (pl.: classid), amelyek nem jellemzőek az e-mailekre
- Kapcsolja ki a CD-ről, floppyról történő rendszerindítást, állítson be BIOS szintű jelszót a módosításokhoz.
- A szerver védelmét erősítse meg, hogy a fertőzés ne juthasson el más szerverekre - vegye igénybe a Szolgáltató rendszeres IDS felülvizsgálat szolgáltatását!
- A vírus ellenőrző programok legyenek minél távolabb a hálózat központjától. Nem elég csupán a kliensek gépein futó vírus ellenőrzés: cél a védelmet minél távolabb elhelyezni a felhasználóktól. Vegye igénybe a Szolgáltató Antivírus megoldásait!
- Maximálja a csatolt állományok méretét, és a megkérdőjelezhető állományokat törölje!
- Maximálja a percenként fogadható, beérkező üzenetek számát!
- Ha szükséges, korlátozza a futtatható fájlok e-mailekhez való csatolását!

- Küldessen a szerverrel üzenetet, ha az furcsa aktivitást észlel. Vegye igénybe a Szolgáltató Port monitorozási szolgáltatását és kapjon SMS üzenetet!
- A backupokat legalább egy hónapig őrizze meg! Vegye igénybe a Szolgáltató Adatmentési Szolgáltatásait!
- Használjon Védett hálózatot. Használjon tűzfalat minden kritikus rendszerhez! A packet-filter használata legyen alapvető, még jobb ha stateful-tűzfalat használ! Gondolkozzon el az alkalmazás szintű tűzfalazás bevezetésének lehetőségéről!
- Oktassa felhasználóit! Ragadjon meg minden alkalmat, hogy az Ön Tudását átadja másoknak!

Tisztában kell lennie azzal, mi jelenthet veszélyt, s egy-egy támadás milyen következményekkel járhat. Nem tehető kizárólag a felhasználó felelőssé a rendszer biztonságáért, főleg nem olyan esetekben, ha a vírusos e-mail, amelyre válaszolt, ismerősétől, kollégájától érkezett (pl.: Melissa vírus), vagy éppenséggel a vírus aktiválásához meg sem kellett nyitni az üzenetet. Ne várja el, és ne is hagyja, hogy a felhasználó biztonsággal kapcsolatos döntéseket hozzon pop-up üzenetekre kattintva.

Utószó

Biztos vagyok benne, hogy Ön nem feltétlenül ért egyet mindennel amit olvasott. Ez esetben kérem, mérlegelje annak a lehetőségét, hogy megfogadja a benne foglaltakat a következő alkalommal, amikor a saját megoldásai kudarcot vallanak. Nagyon valószínű, hogy Ön már birtokában van, volt, számos információnak, tudásnak amelyről említést tettem. Kérem, ez esetben fogadja szavaimat az Ön tudásának megerősítése végett. Abban az esetben, ha Ön új információkat szerzett az idő alatt, amit az olvasásnak szentelt, elértem célomat, Ön megajándékozott a legdrágább kincsével az idejével és figyelmével amit - ez úton is - köszönök!

Véleményem szerint, létezik egészséges paranoia – a kétkedés művészete, avagy a Tudás alapú szkepticizmus része a Tudás alapú társadalomnak!

Kovács Zsolt
Adatpark üzletfejlesztés
Értékesítési vezető

Axelero Internet

Budapest, 2004

Felhasznált irodalom

Deborah Hamdani: Educating the Public. Sans Institute. 2004. March
Galántai Zoltán: A nagy adatrablás. 1998.
Kevin Beaver: Email Management and Security. Realtimpublishers.com, Inc. 2003.
Kevin D. Mitnick: A legendás hacker - a megtévesztés művészete.
(The Art of Deception - Controlling the Human Element of Security.) 2002. ©
Experts: 'Phishing' more sophisticated'. www.cnn.com 2005. január 20.
Http://yikes.tolna.net
Csiff: A vállalatirányítási rendszerek biztonsága 2004. Június 6.
http:// www.biztonsagportal.hu/modules.php?name=Sections&op=viewarticle&artid=9
Csiff: A nélkülözhetetlen kockázatmenedzsment 2004. augusztus 9.
http://www.biztonsagportal.hu/modules.php?name=Sections&op=viewarticle&artid=16
Papp Géza: Social Engineering - avagy az egyik leghatékonyabb hackertechnika pappgeza@tolna.net 2003. Okt. 13
http://www.terminal.hu/artread.php?id=13205710034315

Sy: IT-biztonság: alábecslik az emberi veszélyt sy@terminal.hu 2004. Október 28
http://www.terminal.hu/newsread.php?id=27200909044809
ITTK: Az információbiztonság fenyegetettségének trendjei
http://www.ittk.hu/infinit/2002/0207/index1.html
Dr. Pogányi Gergely: Információ biztonság menedzsment porganyi.gergely@clarity.hu
http://www.clarity.hu/szolgaltat/bodyframe800.php?szcsid=179&szid=112

Köszönet illleti a felsorolt irodalom alkotóit, munkájuk, gondolataik alapvető segítséget nyújtottak az összefoglaló elkészítéséhez! Köszönet illet továbbá mindenkit, aki segítségemre volt e dokumentum elkészítésénél.

Kovács Zsolt, Axelero Internet - 2004 február 9.