18. tétel

malware fogalom

Az angol malware kifejezés az angol malicious software (rosszindulatú szoftver, káros szoftver, kártékony szoftver) összevonásából kialakított mozaikszó. Mint ilyen, a rosszindulatú számítógépes programok összefoglaló neve. Ide tartoznak a vírusok, férgek (worm), kémprogramok (spyware), agresszív reklámprogramok (adware), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (rootkit).

vírusok, férgek, trójai programok

Vírusok Olyan programokat nevezünk vírusnak, melyek képesek reprodukálni, sokszorosítani önmagukat. Működésük, és terjedésük csak bizonyos közegben lehetséges. Ha ez a közeg nem áll rendelkezésre, nem működőképesek. Nem feltétlenül okoznak kárt, sokszor csak kisebb bosszantó tevékenységet művelnek. Működésüknek két ciklusa van. Először megpróbálnak minél jobban elterjedni, minél több gépet megfertőzni, majd egy esemény bekövetkezésekor (például előre meghatározott napon) kifejtik káros tevékenységüket. Ez a tevékenység lehet adatok törlése, felülírása, teljes adatmegsemmisítés, vagy akár fontos programok, menüpontok eltüntetése. Léteznek olyan vírusok is, melyek képesek bizonyos hardvereszközök tönkretételére is.

Férgek A vírusokhoz hasonló programok. Ezek is képesek reprodukálni magukat, de a vírusokkal ellentétben nem szükséges hordozóközeg a terjedésükhöz. Önmagukban, a számítógépes hálózatokat felhasználva terjednek. Manapság a legveszélyesebb programok ebből a típusból kerülnek ki, elsősorban a gyors terjedésük miatt. Mire egy-egy újabb féreg jelenlétét észrevennék, és az ellenszert elkészítenék az erre szakosodott cégek, addig a féreg az internetet használva akár több százezer gépet is képes megfertőzni. Sokféle kárt képes okozni, de már önmagában a terjedéssel is sávszélességet foglal, vagyis az internet egyéb, hasznos forgalmát hátráltatja.

Trójai programok

Olyan programok, amelyek önmagukban nem okoznak kárt, (sőt sokszor hasznos programnak álcázzák magukat) de képesek a háttérben segíteni egyéb ártó szándékú programok bejutását, és működését a számítógépen. Mivel gyakran hasznos programnak mutatják magukat, ezért leggyakrabban a felhasználó tölti azt le számítógépére. Emellett terjedhetnek e-mailben, vagy adathordozókon is.

vírusvédelmi programok

Windows Defender, Avast ,Eset

frissítések szükségessége, frissítések típusai

Fontos a rendszeres frissítés A megfelelően összeállított vírusvédelmi rendszer frissítés nélkül jóformán csak az üzembe helyezés pillanatában tekinthető biztonságosnak, hiszen minden nap újabbnál újabb fenyegetettségeknek van kitéve, rendszeresen jelennek meg ismeretlen "károkozók". Fontos kérdés tehát a rendszer naprakészsége. A vírusadatbázisok frissítése a rendszer hatékonyságának szempontjából kritikus fontosságú, mivel az elektronikus hálózatok korában az új vírusok megjelenése és globális elterjedése között esetenként csupán néhány óra telik el. A vírusadatbázisok rendszeres frissítése ezért kiemelten jelentős feladat, és lehetőség szerint törekedni kell a leggyakoribb, legsűrűbb frissítési lehetőséget nyújtó vírusvédelmi rendszerek alkalmazására. A víruskereső rendszerek frissítésének két vonalon kell megtörténnie: egyrészt a vírusadatbázisoknak

másrészt pedig maguknak a víruskereső programoknak is frissülniük kell. Általánosan a vírusadatbázisok frissítése lényegesen fontosabb és gyakoribb.

SPAM szűrés

A levélszemét (spam) szűrés az informatikai biztonság érdekében végzett rendeltetésszerű működés, melynek során a levelek egyes paramétereik, tartalmi elemeik (szöveges tartalom, további címzettek, levélben szereplő linkek, csatolmányok kiterjesztése, tartalma, stb.)

ismeretlen eredetű levelek és csatolmányainak kezelése

A spam levelek rettentően bosszantóak, vesztegetik az időnket és visszaélnek az erőforrásainkkal. Mindemellett úgy hatolnak be a privát szféránkba, hogy azt senki nem kérte. Kezdetben könnyen lehet, hogy csak szimplán idegesítőek voltak. Ha becsenget hozzánk egy porszívóárus, akkor az valóban lehet idegesítő. De ha minden alkalommal ott áll az ajtónkban, amikor kinyitjuk azt, akkor az már kimeríti a zaklatás fogalmát. Tehát az ilyen tömegesen küldött levelek nem egyszerűen az idegrendszerünknek, hanem a cégünknek és a szélesebb kollektívánknak is sok gondot okoznak. Spam elleni védekezés teljeskörű IT üzemeltetési szolgáltatásunkkal. Épp ezért indult el a spam elleni védekezés világszinten. Számos kezdeményezést ismerünk már, amelyek hatására törvénybe foglalták, hogy a spammelés illegális. Persze a jogalkotás sebessége merőben eltér attól, amilyen gyorsan a spamküldők kidolgozzák újabb és újabb módszereiket. Kezdetben a cégek el sem rejtették a kilétüket, nyíltan felvállalták a tömeges emailek küldését. Így könnyűszerrel lehetett őket tiltani, úgyhogy erre válaszul elkezdték elrejteni személyazonosságukat. Jó megoldásnak tűnt ezután IP cím alapján blokkolni őket, ami egy darabig hatásos is volt. Azonban a spammelők felfedezték, hogy harmadik félen keresztül is kiküldhetik a kéretlen tartalmaikat. Sőt, akár saját domaineket is tarthatnak fent csak spammelés céljából. Minden egyes elolvasott kéretlen levél időt, energiát, erőforrást és pénzt követel a felhasználóktól, de nem csak tőlük. Az internetszolgáltatók, valamint a web- és mailszervereket üzemeltető cégek esetén szintén kézzel fogható financiális következményei vannak a kéretlen leveleknek. Gondoljunk bele: az adatforgalomból elvett sávszélesség, a CPU kihasználása és a tárhelyek üzemeltetése is mind-mind plusz költséget rónak ránk. Ezért kijelenthetjük, hogy lehetetlen minden kéretlen levelet előre szűrni, viszont törekedni kell rá. A rendszergazdáknak és technikai szakembereknek időt és energiát kell arra áldozni, hogy utólag blokkolják a feladókat és foglalkozzanak a kéretlen levelekkel, a spamszűrők és mailszerverek beállításaival és karbantartásaival.

böngésző biztonsági beállításai, privát böngészés

A privát böngészés nem rejti el a személyazonosságát és az online tevékenységét. A weboldalak és az internetszolgáltatók továbbra is gyűjthetnek adatokat a látogatásáról, még akkor is, ha nem jelentkezik be. Ha a munkahelyén használja az eszközt, akkor a cége is figyelheti, hogy milyen weboldalakat keres fel. Ha otthon internetezik, akkor a szolgáltatója és a partnereik is hozzáférhetnek a böngészési tevékenységéhez. Csak egy VPN vagy virtuális magánhálózat, mint például a Mozilla VPN, rejtheti el a tartózkodási helyét, és titkosíthatja online tevékenységét, megóvva személyazonosságát és adatait a kíváncsiskodó szemektől. Ha rejtve szeretne maradni az interneten, próbálja ki a Mozilla VPN(külső hivatkozás) szolgáltatást.

adware, spyware, adathalászat

Ennek egyik formája, hogy egy rosszindulatú weboldal egy másik, jogszerű weboldalnak adja ki magát azzal a céllal, hogy Öntől érzékeny adatokat, csaljon ki, például jelszavát, fiókjának részleteit, vagy

bankkártyájának számát. Az adathalász próbálkozások legtöbbször e-mail üzenetek formájában érkeznek, amik arra próbálják rávenni a címzettet, hogy frissítse korábban megadott személyes adatait egy meggyőzőnek látszó, de hamis weboldalon. További információt talál az Anti-Phishing munkacsoport oldalán és a a Wikipédia Adathalászat szócikke pedig további példákat és eszközöket sorol fel.

Spyware

Spyware-nek, azaz kémprogramnak nevezzük azokat a malware technológiákat, amelyek a felhasználó beleegyezése nélkül adatokat gyűjtenek annak számítógépéről. Az így összegyűjtött adatokat (pl. böngészési preferenciák, gyakran látogatott oldalak) továbbárulják reklámcégeknek vagy más érdekelt harmadik félnek. A spyware vírushoz hasonlóan is terjedhet, de akár egy új program telepítésekor is felkerülhet a számítógépekre. Sőt, a pop-up hirdetések gyakran tartalmaznak ilyen szoftvereket, amelyekre ha a felhasználó rákattint, azok automatikusan installálódnak. A marketing cégek azonban tiltakoztak az ellen, hogy spyware-nek nevezzék ezeket a programokat, ezért a „nagy valószínűséggel nem kívánt programok” elnevezés is forgalomban van. A felhasználó adatait a cookie-k is tárolják, és ha a felhasználó ezzel nincs tisztában, és nem is tájékozódhat erről, akkor ez is spyware-nek minősül. A probléma azonban ezen a ponton már a személyes adatok webes kezelésének kérdésköréhez.

Adware

Az Adware (más néven reklámokkal támogatott program vagy reklámprogram) egy hirdetésre használt szoftver. Telepítés után promóciós tartalmakat jelenít meg többek között felugró ablakok, reklámsávok és szövegközi linkek formájában, azzal a céllal, hogy növelje a hirdetett weboldalak népszerűségét. Az adware-ek fő célja tehát, hogy partnereik népszerűsítésén keresztül bevételt termeljen a fejlesztőknek. A böngészőkhöz hozzáadva azonban az ilyen szoftverek személyes (beazonosításra alkalmatlan) adatokat gyűjthetnek a felhasználó böngészési tevékenységeiről. A begyűjtött adatokat statisztikákhoz használják: a leggyakrabban látogatott weboldalak, a megnyitott hirdetések, az érdeklődési körök stb. feltérképezéséhez. Fontos, hogy az adware-ek általában két csoportba oszthatók: jóindulatúak és potenciálisan kéretlenek. A kéretlen reklámprogramok rendkívül veszélyesek lehetnek, mert érzékeny adatokat is begyűjthetnek. Ebben az esetben a felhasználó akarata ellenére megoszthat például bejelentkezési adatokat, IP-címeket, tartózkodási helyet és más információkat is.