7/2011. SZ. GF UTASÍTÁS A PTE VÍRUSVÉDELMÉRŐL

I. ÁLTALÁNOS RENDELKEZÉSEK

AZ UTASÍTÁS CÉLJA

1.§.(1) Az utasítás célja, hogy elkerüljük az Egyetem számítástechnikai rendszerének a vírusfertőzését, illetve ha a vírusfertőzés már megtörtént, akkor lehetővé váljon az okozott károk minimális szinten való tartása. A vírusvédelmi utasítás kiterjed az Informatikai infrastruktúra vírusvédelmi rendszer kiépítésére, üzemeltetésére, használatára, frissítésére és karbantartására.

AZ UTASÍTÁS HATÁLYA

2.§.(1) Az utasítás tárgyi hatálya kiterjed a PTE Informatikai Igazgatóság által üzemeltetett valamennyi informatikai rendszerre, eszközre, amely felhasználja, feldolgozza, a PTE-nél keletkező, illetve felhasznált adatokat, információkat.

(2) Az utasítás személyi hatálya kiterjed a PTE Rektori Hivatal, GF és KK területen dolgozó minden közalkalmazottjára. A vírusvédelmi utasítás érvényesülését az üzemeltetési környezet megfelelő kialakításával kell biztosítani.

II. ÁTTEKINTÉS

FELELŐSSÉG

3.§.(1) A vírusvédelmi rendszer kidolgozása, szabályozása az Adatbiztonság Felelős feladata, az Informatikai Igazgató, az infrastruktúra üzemeltetésért felelős vezető és szükség esetén külső szakemberek közreműködésével.

A vírusvédelmi rendszer jóváhagyása és hatályba léptetése a Gazdasági Főigazgató hatásköre.

A vírusvédelmi rendszer frissítéséért és karbantartásáért minden egyetemi szervezeti egység esetében a megbízott vírusvédelemért felelős informatikus felel.

A vírusvédelmi utasítás rendelkezéseit a Pécsi Tudományegyetem Rektori Hivatalhoz, GF-hoz és KK-hoz tartozó minden szervezeti egységében végre kell hajtani, az előre meghatározott és rögzített időbeli, térbeli és tárgyi korlátok között.

A felhasználók kötelessége ismerni a víruskereső rendszer használatának fontosságát, betartani a biztonsági előírásokat és követni a vírusvédelemért felelős informatikus, illetve a vírusvédelmi utasítás által megfogalmazott utasításokat.

A rendszert üzemeltetők kötelessége érteni a rendszer működését, gondoskodni annak a szabályrendszerrel összhangban lévő konfigurációjáról, illetve a folyamatos naprakészen tartásról.

KONTROLL PONTOK

4.§.(1) A vírus definíciós fájlok (pattern), vírus engine-ek frissítése megtörtént-e az előírt időközönként.
Hiba esetén az előírt tevékenységek megtörténnek-e (pl vírus napló ellenőrzés)?
A frissítéskor jelentkező hibák javításra kerültek-e?
Incidens esetén az elemzés megtörténik-e?

(2) A fenti tevékenységek dokumentálása az üzemeltetésért felelős osztály feladata, melyet az adatbiztonság felelős ellenőriz ad-hoc módon.

A VÍRUSVÉDELMI UTASÍTÁS ÁLTAL DEFINIÁLT FOGALMAK

5.§.(1) Vírus alatt a továbbiakban a következőket értjük

- olyan kártékony kód, mely a számítógépes rendszerben nem kívánatos módon önmaga sokszorosításáról, szaporításáról gondoskodni tud illetve olyan károkat képes okozni az informatikai rendszerekben, függetlenül attól, hogy az infrastruktúra mely részéről van szó, mely a napi üzemszerű működést megzavarhatja és az Egyetem működésének szempontjából értékes adatokat veszélyeztethet.

A vírusvédelmi rendszer és védelmi mechanizmusok feladata a vírusok felkutatása, működésük aktív, vagy passzív károkozásuk megakadályozása, illetve – lehetőség szerint - megsemmisítésük.

(2)Az „áldozat objektumok" a számítógépes hálózatok azon objektumai, amelyek vírustámadásnak lehetnek kitéve. Ezek az objektumok a mai vírusok képességeit figyelembe véve szinte bármely elektronikusan tárolt adatot jelölhetnek. Ide tartoznak a futtatható programok, a számítógépek indításakor automatikusan betöltött úgynevezett „boot" szektorok, a Microsoft Office programcsomag által használt csaknem valamennyi fájltípus (Word, Excel, PowerPoint, Access, Project), az elektronikus levelek, és általánosan minden olyan elektronikus adathalmaz, amely felhasználható lehet arra, hogy a számítógép által végrehajtható utasításokat hordozza.

Az infrastruktúra üzemeltetési osztályvezető a rendszerek felügyeletéhez, konfigurálásához, karbantartásához és ellenőrzéséhez iránymutatókat ad illetve meghatározza, hogy ezen tevékenységek mily módon kerüljenek elvégzésre általánosságban az összes rendszerben. A vírusvédelemért felelős informatikusi jogköröket a különböző rendszerekben kijelölt informatikusok gyakorolhatják.

(3) A tevékenységek a következőképpen kell, hogy működjenek:

- Az adatbiztonsági felelős irányelveket határoz meg.
- A vírusvédelemért felelős informatikus végzi a feladatait ezen irányelvek alapján, speciálisan az adott rendszer sajátosságait és az alapelveket figyelembe véve.

III. A VÍRUSVÉDELMI FOLYAMAT

6.§.(1)Az előírások első része általánosan, víruskereső rendszertől függetlenül ismerteti a vírusfertőzések megelőzésére, illetve a megtörtént fertőzéskor a károk minimalizálására teendő lépéseket. Az instrukciók külön tartalmazzák a teendőket a felhasználók és a vírusvédelemért felelős informatikus részére.

ÁLTALÁNOS ELŐÍRÁSOK

7.§.(1) A vírusvédelmi rendszerek hatékonyságának három legfontosabb összetevője:

A védelmi szoftvernek jó minőségűnek, a piacon elismertnek és kellő gyakorisággal aktualizáltnak kell lennie, hogy felismerési hatékonysága maximális legyen.

A védelmi szoftvernek minden potenciális támadási ponton aktívan üzemelnie kell. A közvetlenül nem potenciális támadási pontokon üzemelő víruskeresők a rendszer redundanciáját – és ezzel üzembiztosságát – növelik, míg az általános sebességet csökkentik.

A védelmi szoftvernek minden ponton az informatikai infrastruktúrára vonatkozó szabályrendszerrel összhangban álló konfigurációval kell rendelkeznie.

A fenti specifikációnak megfelelően fontossági sorrendben a következő védelmi rétegek kialakítása szükséges:

- A legfontosabb a munkaállomások ellenőrzése, mivel ezek jelentik a vírusok által megcélzott elsődleges támadási felületet. A víruskereső szoftvernek minden lehetséges bejutási pontot ellenőriznie kell (floppylemez, CD-ROM, hálózat, e-mail, különböző USB adattároló eszközök stb.).

- A rendszerben működő fájl- és alkalmazás szerverek másodlagos támadási felületet jelentenek. Védelmük jelentős redundanciát visz a rendszerbe, és feltétlenül ajánlott. A telepített víruskeresőnek – a munkaállomásokon futó változathoz hasonlóan - minden lehetséges bejutási pontot ellenőriznie kell (floppylemez, CD/DVD-ROM, hálózat, e-mail, különböző USB adattároló eszközök stb.), különös tekintettel a szerverek rendeltetésszerű használata közben fellépő adatforgalomra (pl. fájlok forgalmazása, levelezés stb.).

- A tűzfalak és levelező szerverek is másodlagos támadási felületnek számítanak a fájlszerverekhez hasonlóan. A telepített víruskeresőnek – a munkaállomásokon futó változathoz hasonlóan - minden lehetséges bejutási pontot ellenőriznie kell.

ÁLTALÁNOS VÍRUSELLENŐRZÉSI TUDNIVALÓK

8.§.(1) A víruskereső rendszerek két alapvető működési móddal rendelkeznek.

Valósidejű, illetve off-line (passzív) üzemmódban dolgoznak. A valósidejű ellenőrzés feladata a számítógépes rendszer rendeltetésszerű használata közben használatba vett állományok és más objektumok valósidőben, közvetlenül a felhasználás előtt történő ellenőrzése. Ez képezi a rendszer legerősebb védelmi vonalát, és általánosan arra kell törekedni, hogy ez a vonal ne sérüljön, illetve ne menjen át inaktív üzemmódba.

Az off-line, vagy passzív ellenőrzés feladata a teljes állományrendszer átvizsgálása, tekintet nélkül az állományok korára, illetve felhasználásuk gyakoriságára. Ez az üzemmód másodlagos védelmi vonalat képez, redundancia növelő tényező. Alkalmazása feltétlenül szükséges a víruskereső rendszer részeinek, vagy egészének frissítését követően, mivel ez biztosítja a rendszer bővült vírusismeretének azonnali alkalmazását, ezáltal fény derülhet esetleges korábban fel nem ismert, de a rendszert veszélyeztető elemekre.

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, és a vírusvédelemért felelős informatikus feladata.

TERMÉKFÜGGETLEN VÍRUSVÉDELMI ELŐÍRÁSOK FELHASZNÁLÓK SZÁMÁRA

9.§.(1) Aktív védelem

A vírusvédelmi rendszer fő komponense az aktív (tárrezidens, valósidejű) védelem, mely a számítógép működése során állandóan dolgozik. Feladata a felhasználói munka során igénybe vett állományok (programok, adatok, dokumentumok) közvetlenül a használat előtti vírusellenőrzése. Az aktív védelem kikapcsolása tilos!

Amennyiben az aktív védelem nem képes a detektált vírus eltávolítására, nem engedi meg a fertőzött állomány használatba vételét. Ez a normális működés.
Az aktív védelem a vírusvédelemért felelős informatikus által bármely okból történt kikapcsolása esetén a passzív védelem (3. pont) kiemelt jelentőségű és a felhasználók felelőssége szükség esetén azt alkalmazni.

(2) Elektronikus levelezés

Az elektronikus levelezés a vírusok továbbításának leggyorsabb módja, ezért erre külön figyelmet kell fordítani.

A kliens részéről merevlemezre mentett csatolt állományok használatba vételekor az aktív védelem ellenőrzi azt. Ha az állomány fertőzött, arról értesíti a felhasználót. Ha az aktív védelem képes volt a

fertőzés eltávolítására, akkor – a vírusvédelemért felelős informatikus informatív értesítése után – a munka megkezdhető. Ha az aktív védelem nem képes a fertőzés eltávolítására, akkor a fertőzött állomány használatba vételét nem engedélyezi. Ebben az esetben a vírusvédelemért felelős informatikus értesítése szükséges.

Az e-mailben ok nélkül, váratlanul vagy a levél szövegében nem indokoltan érkezett állomány esetében a melléklet tartalmának személyes (pl. telefonos) vagy e-mailben történő ellenőrzése szükséges. Ha a küldő nem szándékosan mellékelt az e-mailhez állományt, akkor semmi esetre sem szabad annak megnyitása és a vírusvédelemért felelős informatikus értesítése elengedhetetlen.

(3) Passzív védelem (off-line ellenőrzés)

A passzív védelem feladata a teljes állományrendszer átvizsgálása, tekintet nélkül az állományok használatba vételére. A víruskereső rendszer frissítésekor ez automatikusan megtörténik.

A passzív védelem futása több percet is igénybe vehet, mivel sok állomány ellenőrzését végzi. Ez a néhány perc azonban esetleg a vírusvédelemért felelős informatikus többórányi (több napnyi) helyreállító munkáját előzi meg. Megszakítani tilos! Lehetőség szerint ez a folyamat a háttérben, a felhasználó számára teljesen láthatatlan módon fut.
A passzív védelem különösen fontos akkor, ha az aktív védelem valamilyen okból deaktivált. Az újbóli aktiválásig a passzív védelem használata a felhasználó feladata és felelőssége, aki köteles minden, a rendszerbe bekerülő adat (pl. pendrive, CD-ROM, e-mail melléklet) ellenőrzését a passzív védelmi rendszerrel azonnal, a felhasználás előtt elvégezni.

VÍRUSVÉDELMI ELŐÍRÁSOK A VÍRUSVÉDELEMÉRT FELELŐS INFORMATIKUS SZÁMÁRA

10.§.(1) A felhasználókra érvényes szabályok a vírusvédelemért felelős informatikusra is vonatkoznak. Az alábbi szabályok ezt egészítik ki.

11.§.(1) Telepítés

A víruskereső rendszer kiválasztása Gazdasági Főigazgatóság és Klinikai Központ területen az adott rendszerben az Infrastruktúra Üzemeltetési Osztályvezető, a Technológiai Referens és az Adatbiztonság Felelős feladata egyéb esetben törekedni kell az egyetemi szintű egységes megoldásra.
A víruskereső rendszerek telepítése (a GF, a KK és a Rektori Hivatal területeken) a vírusvédelemért felelős informatikus feladata (Infrastruktúra Üzemeltetési Osztály).
Az újonnan rendszerbe állított, illetve újratelepített számítógépeken gondoskodni kell a víruskereső rendszer azonnali telepítéséről.
Amennyiben az alkalmazott víruskereső rendszer erre lehetőséget ad, a vírusvédelemért felelős informatikus által a hálózaton keresztül felügyelhető változatokat kell telepíteni. A telepítéskor gondoskodni kell róla, hogy a hálózati adminisztráció során egyértelműen megkülönböztethetők legyenek a különböző gépektől érkező adatok (üzenetek, jelentések, vírusminták, stb.).
A Vírusvédelemért felelős informatikus feladata a telepítéskor a szükséges konfiguráció beállítása, illetve lehetőség szerint gondoskodni arról, hogy a felhasználók önhatalmúlag ne csökkenthessék a vírusvédelmi rendszer működésének hatékonyságát.
A rendszerben található számítógépek naprakész frissítésének biztosításához megfelelő menedzsment eszköz áll rendelkezésre, melynek segítségével minimum hetente egy alkalommal ellenőrizni kell a számítógépek frissítésének állapotát.

12.§.(1) Aktív védelem

A vírusvédelemért felelős informatikusnak joga van az aktív védelem dokumentált módon történő inaktiválására. A dokumentáció tárolása a vírusvédelemért felelős informatikus feladata.

A dokumentálás legalább a következő adatokkal történik:

Dátum,
A kikapcsolást végző személy neve,
A munkaállomás, ahol az aktív védelmet kikapcsolták,
Az inaktiválás oka,
Záradékként az újbóli aktiválás tervezett időpontja, illetve a megtörtént aktiválás tényének rögzítése,
Aláírás.

13.§.(1) Passzív védelem

A passzív védelem jelentősége kiemelt a szerverekkel kapcsolatban. A szerverek vírusellenőrzése másodlagos jelentőségű a munkaállomásokkal szemben. Központi szerepüknél fogva azonban többrétegű ellenőrzés használata szükséges. Ennek keretein belül az aktív védelem használatán túl szükséges a szervereken tárolt adatok rendszeres átvizsgálása. Ezt akkor kell végrehajtani, amikor a szerverek terheltsége minimális (munkaidőn kívül). Ekkor teljes átvizsgálást kell végezni a tárolt állományokon. Az átvizsgálást naplózni kell.

14.§.(1) Frissítések

A víruskereső rendszerek frissítése két vonalon zajlik.

A vírusadatbázisoknak, illetve maguknak a víruskereső programoknak a frissítése. Általánosan a vírusadatbázisok frissítése lényegesen gyakoribb.

A víruskereső programok frissítései CD-ROM-on vagy egyéb online módon (belső központi szerver, internetes oldal, stb.) történnek. Ezen frissítéseknek telepítése az adott rendszer vírusvédelméért felelős informatikus feladata. Akinek tevékenységét a vírusvédelmi utasítással teljes összhangban kell elvégeznie.

A vírusadatbázisok frissítései – gyakoriságuk, kis méretük és nagy számuk miatt – jellemzően elektronikus úton (Internet) érhetők csak el. A rendszeres vírusadatbázis-frissítés az adott rendszer vírusvédeleméért felelős informatikus feladata, melynek gyakorisága 1 nap. Emellett a víruskereső rendszert fejlesztő cégektől érkező figyelmeztetésekre reagálva indokolt esetben az azonnali vírusadatbázis-frissítés is szükséges. Ezen okból célszerű minimum naponta 1 alkalommal automatikus módon ellenőrizni, hogy nem jelent-e meg újabb adatbázis frissítés az Interneten. Ezen kívül célszerű több lehetséges útvonalat felvenni a rendszerekbe, ahol ezen frissítések elérhetők (értsd: Internetes frissítések esetén több letöltő szerver beállítása, ahonnan a frissítések elérhetőek)

Bármilyen, a tágabb értelemben vett víruskereső rendszerben végzett frissítés (azaz adatbázis- vagy programfrissítés) esetén a frissítést végző szakemberek kötelesek gondoskodni arról, hogy az újabb változat azonnali ellenőrzést végezzen minden védett számítógépen.

VÍRUSFERTŐZÉS

15.§.(1) A víruskeresők a fertőzés tényének kimutatása után a konkrét vírusok karakterisztikájától függően képesek vagy sem a fertőzések eltávolítására. Amennyiben a fertőzés eltávolítható, úgy célszerű a fertőzött állapotot további analízis céljából archiválni (kontrollált környezetben), majd a fertőzést eltávolítani. Amennyiben a fertőzés automatikusan nem távolítható el, úgy a fertőzött állományt használatra alkalmatlanná kell tenni (Ez leggyakrabban az állomány ún. kiterjesztésének megváltoztatásával érhető el, mivel így annak tartalmára a rendszer következtetni nem tud. Jó megoldás még a vírusok „karanténba" zárása, azaz a felhasználók által nem elérhető helyre történő mozgatása is.). Ha az állomány tartalma mentésből nem állítható helyre (ez egyébként az Egyetemen alkalmazott mentési rendszer hiányosságaira is utalhat), úgy a víruskereső gyártóját kell felkeresni további segítségért. A fertőzött állományt a fertőzött állapotában kell a szakértőkhöz eljuttatni. Az állományok előzetes módosítása, illetve a megfelelő szakértelmet és tapasztalatot nélkülöző helyreállítási kísérletek jelentősen csökkenthetik a sikeres helyreállítás esélyét, ezért az ilyen jellegű tevékenységek szigorúan tilosak!

VÍRUSGYANÚ

16.§.(1) A víruskeresők képesek lehetnek új, eddig ismeretlen vírusok, illetve ismert vírusok módosított változatainak detektálására. Az is előfordulhat, hogy a víruskereső egyáltalán nem detektál semmilyen vírust, azonban a rendszer normális működésében bekövetkezett változások egy új fertőzés gyanúját erősítik. Ilyen esetben – a további fertőzés megállítása, illetve a fertőzött adatok fertőtlenítése érdekében – kiemelt fontosságú a vírusmintáknak a fejlesztőkhöz történő eljuttatása. A vírusok analizálása nem a vírusvédelemért felelős informatikus feladata.

(2) A vírusminta-küldés általános szabályai:

A vírusminta-küldés a vírusvédelemért felelős informatikus feladata.

Legelőször is, ha ez elvégezhető, el kell különíteni a fertőzött állományokat, hogy esetleges új vírusok esetén a további fertőzések megakadályozhatók legyenek.
A mintaként küldendő állomány(oka)t gondosan ki kell választani: ha több is van belőle, akkor 2-3 eltérő tulajdonságokkal (méret, típus, stb.) rendelkező mintát kell választani. Ha a fertőzés megléte nem egyértelmű, akkor lehetőleg a 2-3 leggyanúsabb állományt kell választani. Ajánlott ehhez szakértő segítségének igénybevétele (telefonon).
Vírusmintát e-mailben, nyílt formában szigorúan tilos küldeni. Legalább tömöríteni kell az állomány(oka)t, de a legjobb, ha valamilyen titkosítást is alkalmaznak. Ezzel elejét lehet venni annak, hogy az új vírus véletlenül továbbterjedjen.

A vírusmintával együtt feltétlenül mellékelni szükséges a fejlesztők számára egy rövid, tömör tájékoztatót.

Ennek a következőket kell tartalmaznia:
Hibajelenség leírása, vagy a víruskereső program által küldött üzenetek (szöveges formában, NEM képernyőképként).
A víruskereső program verziószáma
Annak megjelölése, hogy a mintaként küldött adatok mekkora fontossággal bírnak
A küldő neve, elérhetősége
A vírusminta-állomány neve legyen minél jellemzőbb: kerülendő az általános elnevezések használata (pl. VIRUS.ZIP, MINTA.ARJ). A vírusokat analizálóknak ez komoly gondot jelenthet. Az állomány neve legyen pl. XXÉÉHHNN.ZIP, ahol XX a cég nevéből néhány karakter, ÉÉHHNN pedig a dátum, amikor a mintát vették.

Vírusmintát CSAK kifejezetten víruskutatással foglalkozó szakembereknek szabad küldeni. Kerülni kell a vírusminta terjesztését. Illetéktelen személyek kezébe kerülve a vírus elterjedésének valószínűsége nő.

Tilos mintát levelező csoportoknak, hírcsoportoknak küldeni!

RENDSZERENKÉNT ELKÉSZÍTENDŐ DOKUMENTUM FŐ TÉMÁK

17.§.(1) **A rendszerenként elkészítendő vírusvédelmi dokumentumok fő témái kötelezően a következők kell, hogy legyenek:**

- Az adott rendszernél használt vírusvédelmi rendszer felépítése. Leírással, ábrával
- A rendszer frissítése milyen módon történik (leírás, ábra)
- A rendszer működését, a frissítéseket ellenőrző felület bemutatása (menedzsment konzol)
- A vírusellenőrzés milyen gyakorisággal és milyen házirenddel (policy) történik meg az adott rendszerben
- Vírus gyanú / fertőzés esetén milyen munkafolyamatot szükséges elvégezni adott rendszeren
- Felelősségek, tevékenységek, ellenőrzések (általánosságban).

VÍRUSVÉDELMI UTASÍTÁS TÉMÁI RENDSZERENKÉNT

18.§.(1) Minden rendszer vírusvédelmének alapja jelen dokumentum kell, hogy legyen.

Minden rendszerben egyedi dokumentáció készül a vírusvédelemmel kapcsolatban, melyben a következő témákra kell minden esetben kitérni és dokumentálni:

- Minden az eljáráshoz kapcsolódó dokumentumban megfogalmazottaktól való eltérés és annak oka (amennyiben van ilyen),
- konkrét munkafolyamatok,
- felelősségek,
- tevékenységek,
- ellenőrzések dokumentálása

KAPCSOLÓDÓ DOKUMENTUM

19.§.(1) Vírusvédelmi utasítás 1. számú melléklete (üzemeltetői munkatársak részére, IT belső használatra).

IV. ZÁRÓ RENDELKEZÉSEK

HATÁLYBA LÉPÉS

20.§.(1) Az utasítás 2011. november 11. napján lép hatályba.

(2) Az utasítás szakmai tartalmáért (előkészítéséért, előterjesztéséért, aktualizálásáért, és évenkénti felülvizsgálatáért) az Informatikai Igazgatóság vezetője felelős.

(3) A végrehajtással kapcsolatban további tájékoztatást nyújt, illetve az utasítás előírásai betartásának ellenőrzéséért felelős az Informatikai Igazgatóság.

Dátum, 2011. november 09.

Krutki Józsefné dr.

gazdasági főigazgató

PÉCSI TUDOMÁNYEGYETEM * GAZDASÁGI FŐIGAZGATÓSÁG 6.