DATORSISTĒMU DROŠĪBA
COMPYTER SYSTEMS SECURITY

Autors: **Anna Kubarenko**, e-pasts: annarogozina14@gmail.com, +37128358730
Zinātniskā darba vadītājs: **Pēteris Grabusts, Dr.sc.ing.**, e-pasts: peteris.grabusts@rta.lv
Rēzeknes Tehnoloģiju akadēmija, Atbrīvošanas aleja 115, Rēzekne, Latvija

Abstract. *The author in this work provides insight into computer systems security. Themes which are discussed is hardware security, logical security, viruses and computer protection. Nowadays computers are a part of daily life, so each user how to know how to protect computer and its data.*

Keywords: *computer security, hardware security, logical security, viruses*

Ievads

Attīstoties laikam un tehnoloģijām, pieaug datu un datorsistēmu apjoms un sarežģītība. Šis aspekts ir radījis neizbēgamu saskarsmi ar problēmām, kas tiešā veidā ir saistītas ar to, kā pareizi uzturēt sistēmas, kā nodrošināt tās attiecīgu un piemērotu darbību. Jebkura datorsistēma balstās uz vairākiem pamatelementiem: datortehnika un firmas, kas to piegādā, programmnodrošinājums un firmas, kas to izstrādā, cilvēki, kuri šo datorsistēmu apkalpo un lieto. Datorsistēmas lietotājam parasti neinteresē, kā sistēma darbojas, bet ir būtiski, lai tā spētu nodrošināt šādu prasību izpildi:

- Datorsistēma ir spējīga jebkurā brīdī izpildīt lietotāja uzdevumu;
- Uzdevums tiek veikts tā, kā tas ir paredzēts specifikācijās;
- Datorsistēmas darbības rezultāti ir pieejami tikai autorizētiem lietotājiem;
- Datorsistēmas darbība jebkurā brīdī ir paredzama.

Visas šīs prasības apzīmē ar terminu "informatīvo sistēmu drošums" (ISD). Ar terminu "informatīvo sistēmu drošība" parasti saprot sistēmu un informācijas aizsardzības reglamentējošo prasību kopumu. Informatīvo sistēmu drošības principi pieprasa nepārtrauktu vadības kontroli pār tās pārvaldījumā esošo datortehniku, datu ievadu, izvadu un apstrādi, vienlaikus nodrošinot un kontrolējot informācijas izmantošanas autorizāciju. Visus ar informatīvo sistēmu drošību saistītos jautājumus var iedalīt divās lielās grupās: datorsistēmu fiziskā drošība un datorsistēmu loģiskā drošība.

Īss skaidrojums

Datorsistēmu fiziskās drošības paaugstinošie pasākumi nodrošina aizsardzību pret datu zudumiem, kurus var radīt fiziska rakstura bojājumi: datortehnikas bojājumi, strāvas zudumi vai tās zemā kvalitāte, sakaru līniju bojājumi, stihiskās nelaimes, zagļi utt. Datorsistēmu fizisko aizsardzību veic ar speciālām iekārtām (dublējošās iekārtas, UPS, signalizācija, novērošanas iekārtas), kā arī speciālu kontrolējošu administratīvo reglamentu palīdzību.

Datorsistēmu loģisko drošību nosaka sistēmas aizsardzība pret programmu nepareizu darbību (kļūdas programmnodrošinājumā, datorvīrusi) un cilvēku mērķtiecīgu vai kļūdainu darbību (uzņēmuma darbinieki, nelabvēļi utt.).

Datorsistēmu fiziskā drošība

Datora fiziskā drošība ir atkarīga no tā iekšējo komponentu drošības: procesora, atmiņas, barošanas avota utt. Jebkuras datora iekārtas vai komponenta atteikums darba laikā droši vien novedīs līdz visa datora atteikumam darboties. Labākā gadījumā dators būs jāpārstartē, sliktākajā gadījumā var pazust dati un vēl sliktākajā gadījumā var rasties kļūda datos, ko lietotājs nevar pamanīt, un tās sekas parādīsies tikai daudz vēlāk.

http://dx.doi.org/10.17770/het2016.20.3547

Datora strāvas apgāde. Būtisks drošības elements, it īpaši izdalītiem serveriem. Ja kaut kāda iemesla tiek atslēgta elektrība, tad parasts lietotājs pazaudēs pusstundas vai stundas darba rezultātus. Ja pazūd strāvas piegāde bankas lokālā tīkla vai Internet serverim, tad to izjutīs desmitiem un pat tūkstošiem lietotāju, kuri ir pieslēgušies pie konkrētā servera. Datorsistēmu drošību var ietekmēt arī telpu stāvoklis. Jautājumi ir vairāki. Kādam personu lokam ir piekļūšana pie darba stacijām un serverim? Kur un kādā veidā tiek glabāti datu nesēji? Kāda temperatūra un mitrums ir darba telpās, kur atrodas datori? Cik kvalitatīva ir elektrības instalācija telpā un visā ēkā? Datorsistēmu fiziskās drošības aspektu ir ļoti daudz. Parasti tiek izstrādāti noteikti normatīvie dokumenti, kas reglamentē šīs prasības gan attiecībā uz pašiem datoriem, gan attiecībā uz to vidi, kur datori tiek novietoti. Kā jau iepriekš minēts, datora kopīgais drošums ir atkarīgs no tā sastāvdaļu drošības. Datora procesora darbības drošība ir atkarīga no temperatūras, jo mūsdienu datoru procesori strādā ļoti augstās darba frekvencēs un ir izteikta sakarība starp procesora darba frekvenci un siltumu, ko tas izdala darba laikā. Lai procesors nepārkarstu un nesakustu, to dzesē ar ventilatoru, kas ir piestiprināts pie paša procesora. Ja kaut kāda iemesla dēļ ventilators apstāsies vai nespēs pietiekami labi dzesēt datora procesoru, tad dažu sekunžu laikā procesors pārkarsīs un sabojāsies. Mūsdienu datori ir apgādāti ar iekšējo termisko aizsardzību, kas atslēdz procesoru, ja tā temperatūra pārsniedz kritisko. Šāda aizsardzība pasargā procesoru no bojājuma. Jebkurā gadījumā dators pārstās darboties. Ja lokālā datortīkla servera telpā ir paaugstināta temperatūra, tad tas var ietekmēt servera un līdz ar to visa datortīkla drošību. Ir jāatceras, ka jebkuram datoram, tāpat kā jebkurai elektroniskai ierīcei pastāv cieša sakarība starp tās temperatūru un drošību. Un šī sakarība liek sevi manīt karstos vasara mēnešos, kad datoru "uzkāršanās" varbūtība strauji pieaug tieši paaugstinātās temperatūras dēļ.[1]

Jebkuras elektroniskās ierīces darbību var traucēt arī paaugstināts gaisa mitrums. Šī problēma nav tik aktuāla kā temperatūras režīms, bet jāatceras, ka mitrums palielina strāvas noplūdes elektroniskās iekārtās, kas var izraisīt īssavienojumus un bojājumus. Viens no būtiskajām datora komponentiem, kas ietekmē datora drošību kopumā, ir datora operatīvā atmiņa. Operatīvajā atmiņā atrodas operētājsistēmas kodols, lietotāju programmas un apstrādājamie dati. Katrs baits sastāv no astoņiem bitiem un kļūda jebkurā bitā var izraisīt visdažādākās sekas. Ja kļūda ir attēlā, kas tiek apskatīts Internet pārlūkprogrammā, tad šo kļūdu lietotājs pat nepamanīs, ja kļūda ir operētājsistēmas kodolā, tad sekas būs katastrofālas. Kļūdas operatīvajā atmiņā ir nopietna problēma, ar kuras risināšanu nodarbojas jau kopš pirmo mikrodatoru parādīšanās. Viena no svarīgākajām datora iekārtām ir diski. Aplūkojot datora drošības jautājumus, parasti izskata tikai cieto disku drošības pakāpi. Attiecībā uz diskiem izšķir divus gadījumus: darba stacijas un serveri. Darba stacijās vai personālajos datoros parasti ir tikai viens cietais disks. Cietā diska stabilu darbu var ietekmēt vairāki faktori. Ņemot vērā, ka ieslēgtam datoram cietais disks visu laiku griežas (izņemot gadījumu, kad datora cietam diskam ir uzlikts aiztures laiks, pēc kura tas automātiski apstājas, ja ilgāku laiku nenotiek nekādas darbības ar disku), strādājošo datoru nav ieteicams kustināt un ir jāizvairās no vibrācijas un sitieniem. Ir jāatceras, ka ikviens cietais disks ir ļoti precīzs mehānisms, kura precizitātes raksturīgākie izmēri ir mērāmi mikrometros. Tāpēc ar cietajiem diskiem jārīkojas ļoti uzmanīgi. Diskos ierakstītie dati ir aizsargāti ar kļūdu labojošiem kodiem (parasti tie ir Hemminga kodi) un tāpēc datu kļūdu varbūtība ir ļoti niecīga. Pašlaik uzskata, ka datora cietā diska drošības pakāpe ir diezgan augsta un pilnīgi apmierina darba stacijas drošības prasības. Ja apskata cieto disku izmantošanu failu vai Internet serveros, tad viena atsevišķa cietā diska kļūdas varbūtība ir jau vērā ņemams faktors un ir jāparedz situācijas, kad cietais disks pārstāj darboties. Var gadīties arī diska fiziskie bojājumi, jo tā ir mehāniskā ierīce. Problēmu risina šādi: veido cieto disku masīvu, kas sastāv no vairākiem vienādiem cietiem diskiem. Lielajos failu serveros izmanto pazīstamu RAID (*Redundant Array of Independent Disks*) sistēmu.[2] RAID sistēma uzlabo drošību, bet dažreiz zaudē ātrdarbībā. RAID sistēmas darbības principi ir šādi:

- Vairāki fiziskie diski tiek uztverti kā viens loģiskais disks;
- Ierakstot datus loģiskā diskā, tie tiek ierakstīti vairākos fiziskos diskos;
- Sistēmai ir vairāki līmeņi: RAID 0, 1, 2, 3, 4, 5;
- Neizslēdzot datoru, var nomainīt bojātu disku (dažiem RAID līmeņiem);
- Viens vai vairāki diski tiek definēti kā rezerves diski, ar kuriem var aizstāt bojātu fizisko disku (dažiem RAID līmeņiem).

RAID sistēma var būt izmantota serveros un darba stacijās ar dažādām operētājsistēmām, tādas kā: *Novell Netware, Windows NT Workstation/Server, OS/2 Warp Server Advanced, UNIX*. RAID sistēma sastāv no vadības programmas vai kontroliera un cieto disku masīva. Dārgākās sistēmās izmanto speciālu RAID vadības kontrolieri, kas nodrošina darbu ar masīva diskiem fiziskajā un loģiskajā līmeņos. Šajā gadījumā var panākt maksimālu disku ātrdarbību. Operētājsistēma strādā ar RAID kā ar vienu loģisko disku. Ierakstāmo un nolasāmo datu kontroli un kļūdu labošanu, ja tāda ir paredzēta, nodrošina iepriekš minētais RAID kontrolieris. RAID sistēmas darbības princips atšķiras ar dažādiem RAID līmeņiem. Pašlaik visbiežāk izmanto RAID5 sistēmu. Raksturojot RAID5 sistēmu kopumā, ja kādā diskā ir kļūda, tad tā tiek izlabota, ja kļūda ir vienlaikus vairākos diskos, tad tā tiek uzskatīta kā nopietna kļūda un sistēma var būt nobloķēta, bet šāda dubultas kļūdas varbūtība ir ārkārtīgi maza. Ja kāds disks ir bojāts fiziski, tad tā vietā automātiski tiek pieslēgts rezerves disks. Izmantojot pārējo disku paritātes informāciju, rezerves diskā tiek ierakstīti pazudušie dati. Bojāto disku var izņemt no datora un nomainīt, neapturot datora darbību.
RAID sistēmas ir spējīgas nodrošināt nepārtrauktu datora darbību. RAID tiek izmantots gadījumos, ja ir paaugstinātas prasības sistēmas drošībai.

Datorsistēmu loģiskā drošība

Datorsistēmu loģiskā drošība paredz pasākumu un līdzekļu kopu, kas vērsta pret programmu un cilvēku nepareizu vai neatļautu darbību. Pasākumus, kas ir vērsti pret cilvēku (arī darbinieku) nepareizu, kļūdainu vai kaitniecisku mērķtiecīgu darbību, var iedalīt šādos virzienos:

- Lokālā tīkla izdalīto serveru aizsardzība;
- Lokālā datortīkla darba staciju aizsardzība;
- Lokālā datortīkla slūžas jeb vārtu datora aizsardzība, jo caur šo datoru notiek sadarbība ar citiem lokāliem tīkliem vai Internet tīklu;
- Datu rezerves kopiju veidošana.

Programmu darbība arī var ietekmēt datorsistēmas drošību. Var pieminēt šādus aspektus:

- Datorvīrusu izraisītie datu zaudējumi;
- Kļūdas programmnodrošinājumā, sākot ar lietojumu programmām un beidzot ar operētājsistēmām.[3]

Datorsistēmu vīrusi

Par datorvīrusu sauc programmu, kas datorsistēmā veic noteiktas darbības, kuras nav vajadzīgas lietotājam (bieži vien kaitīgas) un par kurām lietotājs neko nezina. Pastāv divas galvenās vīrusu pazīmes:

- Vīruss spēj sevi reproducēt, patstāvīgi vairoties;
- Vīruss spēj savu reprodukciju pievienot citiem, parasti programmu failiem.

Ir pazīstami gadījumi, kad datorvīruss ir dezorganizējis lielu datortīklu sistēmu valsts līmenī, kad vīrusa dēļ nestrādāja tūkstošiem datoru un kad finansiālie zaudējumi tiek rēķināti miljonos dolāru. Pašlaik ir zināmi vairāk nekā 40000 vīrusu, pie tam katram vīrusu paveidam ir tikai tam raksturīgās pazīmes. Izšķir galvenos vīrusu darbības virzienus:[4]

- Noteiktu sistēmas vai gadījuma failu bojāšana;

- Disku sistēmas apgabalu, *boot* sektora, failu sadalījuma tabulas (FAT) bojāšana, kas parasti izraisa smagus cietā diska datu bojāšanu;
- Sistēmas darba gaitas palēlināšanās;
- Sistēmas "uzkāršana";
- Programmas normālas darbības traucēšana;
- Dažādu ziņojumu izvadīšana, kas neattiecas uz sistēmu.

Pastāv divas lielās grupas, kurās var iedalīt vīrusus – parastie un rezidentie vīrusi. Parastie vīrusi ir aktīvi tad, kad ir aktīvs inficētais fails vai programma. Daudz bīstamāki ir rezidentie vīrusi, kas visu laiku atrodas datora operatīvajā atmiņā. Kad vīruss tiek ielādēts atmiņā, tas pārņem operētājsistēmas vadību un turpmākā rīcība ir atkarīga jau no vīrusa izpausmes veida. Lai izvairītos no jaunākajiem vīrusiem, ir jāieinstalē antivīrusa programmnodrošinājumu, tādu kā, piemēram, *Norton Antivirus, McAfee VirusScan* vai *Dr.Web*. Pie tam nevajag aizmirst par vīrusu datubāzes atjaunošanu, jo jaunākie vīrusi parādās gandrīz katru dienu.[5]

Summary

As computing systems become more essential to our daily lives, it becomes ever more important that the services they provide are available whenever we need them. We must also be able to rely on the integrity of the systems, and thus the information that they hold and provide. We want to be assured that they will work exactly as expected, and that they will keep working – even in the face of disasters, accidents, or deliberate attempts to interfere with or prevent their function.

Computer security can takes two forms. Software security provides barriers and other cyber-tools that protect programs, files, and the information flow to and from a computer. Hardware security protects the machine and peripheral hardware from theft and from electronic intrusion and damage.

Logical Security consists of software safeguards for an organization's systems, including user identification and password access, authenticating, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation. It is a subset of computer security.

A computer virus is a malware that, when executed, replicates by inserting copies of itself into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as acquisition of hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, logging their keystrokes, or even rendering the computer useless. However, not all viruses carry a destructive payload or attempt to hide themselves the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without user consent.

Secinājumi

Veicot informācijas apkopošanu un analīzi, var secināt:

- Datorsistēmas drošība galvenokārt ir atkarīga no cilvēkiem, kuri strādā ar viņu, bet datortīkla drošība ir atkarīga no administratora, kurš uztur datortīklu;
- Nekad nevar atpalikt no pēdējām ziņām datortīklu drošības jautājumos, jo tas var ietekmēt datorsistēmas drošību;
- Pirms iegādāties jaunu programmnodrošinājumu, jāuzzina visu par to, jāatrod informācija, tikai tad var izlemt par pirkumu;
- Serverus jāuzstāda drošās vietās, kur nav pieejama svešu cilvēku pieeja, jābūt labai signalizācijai. Nevajag pieslēgt klaviatūru un displeju, pie servera ir jābūt pieejai tikai caur tīklu;

- Labāk paturēt pie sevis informāciju, kā darbojas datortīkla drošības elementi, jo mazāk ir zināms nelabvēlim, jo labāk;
- Regulāri ir jāpārbauda failus, jo tajos var atrast kādas programmas vai hakera darbības atspoguļojumu;
- Uz servera ir jābūt uzstādītai labi aizsargātai operētājsistēmai;
- Vienmēr ir jābūt uzstādītiem programmnodrošinājuma labojumiem, pretvīrusu atjauninājumiem;
- Jācenšas maksimāli samazināt datortīkla izmēru, un bez liekas vajadzības nepieslēgt to Internet tīklam.
- Ugunsmūra (*Firewall*) izmantošana palīdz uzturēt datortīklu kārtībā, neļauj hakeriem piekļūt pie aizsargātiem datiem.

Literatūra

1. http://drossinternets.lv/page/60
2. https://www.cert.lv/section/show/11
3. https://datoradrosiba.wordpress.com/
4. http://www.r60vsk.lv/materiali/M6/drosiba6-lv.pdf
5. Drošība internetā: praktiski ieteikumi un noderīgi padomi / red. Linda Zemīte ; Rīga : Zvaigzne ABC, [2009]. 64.-65.lpp