



Mājas datora aizsardzība

Efektīvas aizsardzības pamatprincipi

Lai efektīvi pasargātu mājas datoru no tādiem plaši izplatītiem apdraudējumiem kā būtiskas informācijas (kredītkaršu numuri, tiešsaistes spēļu kontu pieejas dati utt.) zādībām vai tā saucamās „zombēšanas”, kad dators tiek inficēts ar īpašām kaitīgām programmām tā izmantošanai surogātpasta sūtīšanā, datokrāpniecībā un citos kibernoziegumos, ir nepieciešams veikt daudz aizsardzības pasākumus. Ir būtiski, lai lietotājs būtu pazīstams ar efektīvas aizsardzības pamatprincipiem.

1. Efektīva aizsardzība pamatojas uz pareizi izvēlētu līdzsvaru starp risku un izmantotajiem aizsardzības līdzekļiem un pasākumiem.

Diemžēl reālajā dzīvē 100% drošība nav iespējama, tā var tikai būt tuvu šim rādītājam. Tāpēc, rūpējoties par datora drošību, lietotājam nākas risināt uzdevumu – kādi līdzekļi un pasākumi būtu nepieciešami, lai iespējami samazinātu risku.

Vieglāk to būs saprast, skatot pavisam vienkāršu piemēru ar parolēm, ko mums nākas izmantot ikdienā. Izvēloties tādas pavisam vienkāršas un viegli uzminamas paroles kā 1234 vai *qwerty*, mēs neapšaubāmi pakļausim mūsu informāciju vai datorsistēmu nepamatoti lielam riskam. Savukārt parole, kas izveidota ar īpašu utilitārogrammu palīdzību, piemēram, *MWD9!3Yowd913Yo*, nodrošinās ļoti augstu drošību, tomēr var būt grūti lietojama un daudzos gadījumos arī pārlietu gara. Visdrīzāk, ka vidēja svarīguma parolei būs pilnīgi pietiekami ar astoņiem simboliem, un to var izveidot no pašam lietotājam būtiskas informācijas, kas sakombinēta pēc viņam viegli iegaumējamiem pamatprincipiem, piemēram, zilsmakonis.

2. Efektīva aizsardzība ir pastāvīgs process un nevar tikt realizēta ar vienreizējiem kampaņveida pasākumiem.

Nekas nestāv uz vietas – attīstās gan apdraudējumi, gan aizsardzības līdzekļi. Programmatūrā katru dienu tiek atklātas drošības nepilnības un laisti klajā tās atjauninājumi. Tie ir tikai daži iemesli, kāpēc par sava datora drošību būtu jārūpējas ikdienā. Par laimi, lielākā daļa tādu procesu kā antivīrusu datubāzu un programmatūras atjaunināšana mūsdienās parasti ir automatizēti. Tomēr lietotājam būtu jāparūpējas un jāseko, lai visas šīs automātiskās atjaunināšanas iespējas tiešām tiktu izmantotas.

3. Efektīva aizsardzība ir komplekss, kurā ir daudzi līdzekļi un pasākumi.

Pagājušā gadsimta deviņdesmitajos gados liela daļa datoru lietotāju antivīrusu programmatūru uzskatīja drīzāk par tādu kā ekskluzīvu līdzekli un ieinteresējās par to tikai tad, kad tika konstatēta datora inficēšanās. Situācija krasi mainījās pēc pirmajām datorvīrusu masveida epidēmijām, kuru rezultātā tika zaudēti dati, – antivīrusu programmatūra strauji kļuva par obligātu datorā instalējamās programmatūras daļu. Turpmākā datorvīrusu un kibernetikas attīstība parādīja, ka internetam pieslēgtam datoram tikpat obligāts ir uguns mūris, bet e-pasta lietošana nav iedomājama bez pretsurogātpasta programmas. Tomēr arī šie līdzekļi dažos gadījumos mūsdienu agresīvajā interneta vidē var izrādīties bezspēcīgi, ja līdzās ar tiem savlaicīgi netiek atjaunināta programmatūra, lietotājs nezināšanas vai nolaidības dēļ ignorē elementāru piesardzību, operētājsistēmai nav veikti iestatījumi, kas paaugstina drošību utt.

Aizsardzības sistēmas daļas

Datorsistēmas aizsardzības sastāvdaļas nosacīti var iedalīt tehniskajos līdzekļos un pasākumos. Pie tehniskajiem līdzekļiem pieskaitāma aizsardzības programmatūra un aparātiskie aizsardzības līdzekļi – uguns mūri, antivīrusi utt. Pie pasākumiem – programmatūras atjaunināšana, nepieciešamo drošības iestatījumu veikšana, lietotāja izglītošanās utt.

Uguns mūris

Jebkura internetam pieslēgta mājas datora aizsardzība nav iedomājama bez uguns mūra. Uguns mūris var būt realizēts programmatūras vai aparatūras veidā. Pēc būtības jebkurš uguns mūris ir noteikumu (*rule*) kopums, kas tiek piemērots datora aizsargājamā datora komunikācijām ar „ār pasauli”.

Uguns mūris var būt personālais – tāds, kas aizsargā vienu konkrētu datoru, vai centralizētais, kas aizsargā veselu tīklu, piemēram, mājas lokālo datortīklu. Personālā uguns mūra gadījumā tajā iekļautie noteikumi var attiekties ne tikai uz datora, bet arī konkrētu uz lietojumprogrammu komunikācijām, kas nodrošina papildu aizsardzību. Tā, piemēram, ar uguns mūra palīdzību atļaujot komunikācijas ar internetu tikai tām lietojumprogrammām, kam tas nepieciešams, mēs varam nopietni mazināt datu zādzības iespēju.

Personālie uguns mūri parasti tiek realizēti programmatūras veidā un mēdz būt gan kā atsevišķas programmas, gan kā daļas tā saucamajās „Internet Security” programmatūras paketēs. Taisnības labad jāpiebilst, ka personālais uguns mūris ir iebūvēts *Windows* operētājsistēmās *Windows XP SP2* un *Windows Vista*. Diemžēl šo uguns mūru funkcionalitāte un aizsardzības spējas, kā ir pierādījis neatkarīgos testos, būtiski atpaliek no trešo ražotāju izstrādājumu snieguma.

Centralizētie uguns mūri parasti ir iekļauti mājas lokālo datortīklu maršrutētājos, kas ļauj interneta pieslēgumu sadalīt vairākiem mājas datoriem.

Antivīruss

Antivīrusu programmatūras, galvenā funkcija ir identificēt kaitīgās vai potenciāli kaitīgās programmas un nepieļaut vai pārtraukt to darbību datorā. Kaitīgo programmu (datorvīrusi, Trojas

zirgi, reklāmas/spiegošanas programmatūra utt.) identifikācija tiek veikta ar dažādām metodēm – signatūru salīdzināšanu, heuristisko analīzi, uzvedības bloķēšanu u. c.

Signatūru metode ir vecākā no antivīrusos izmantotajām un ļauj (līdzīgi kā cilvēkus ar pirkstu nospiedumu palīdzību) identificēt kaitīgās programmas ar iepriekš sagatavotu signatūru jeb neliela apjoma koda paraugu palīdzību. Šī metode ļauj ļoti precīzi noteikt konkrētas kaitīgās programmas, kas jau nokļuvušas speciālistu rokās un kurām jau izstrādātas signatūras.

Diemžēl signatūru metode mūsdienu apstākļos viena pati nespēj nodrošināt pietiekamu aizsardzību, jo laika posmā, kamēr kaitīgās programmas paraugs nokļūst pie antivīrusu speciālistiem, kamēr tas tiek analizēts, kamēr tiek izstrādāta un izplatīta signatūra, var ciest ļoti daudzi interneta lietotāji.

Lai pasargātu interneta lietotāju datorus no inficēšanās ar vēl nezināmām jaunām kaitīgajām programmām, antivīrusos tiek lietota heuristiskā analīze un arvien biežāk arī uzvedības bloķēšana. Ar pirmās palīdzību tiek analizēts kods, lai konstatētu aizdomīgu komandu secības, bet ar otrās palīdzību tiek sekots līdzī, vai programmu darbībā datorā nav konstatējama uzvedība, kas vienāda ar kaitīgu programmu uzvedības modeļiem. Jāpiebilst, ka antivīrusu tehnoloģijās popularitāti gūst arī tā saucamie emulatori, kas paredzēti automātiskai datorprogrammu darbības pārbaudei īpašā virtuālā vidē pirms to darbības „reālā” lietotāja datorā.

Taču arī šīs metodes nav bez trūkumiem – tās spēj tikai ar augstāku vai zemāku varbūtību „izteikt aizdomas” par pārbaudāmā faila kaitīgumu. Tāpēc praktiski visi mūsdienu antivīrusi iekļauj signatūru metodi kopā ar heuristisko analīzi, bet tehnoloģiski attīstītākie arī uzvedības bloķētāju un emulatoru.

Visas antivīrusos izmantotās aizsardzības metodes prasa regulāru atjaunināšanu – signatūru metode ļoti bieži (līdz pat vairākām reizēm diennaktī), bet pārējās – retāku. Atkarībā no antivīrusā izmantojamām kaitīgo programmu noteikšanas metodēm, to izpildījuma kvalitātes un atjauninājumu biežuma dažādu ražotāju aizsardzības produktu aizsardzības spējas var būt ļoti atšķirīgas.

Vēsturiski ir izveidojusies situācija, ka līdzās antivīrusu programmām ir attīstījusies atsevišķa **pretspiegošanas (*anti-spyware*)** aizsardzības programmu klase, kas pēc galvenajiem darbības principiem ne ar ko neatšķiras no antivīrusiem. Sākotnēji šī aizsardzības programmu klase bija paredzēta reklāmas programmatūras (*adware*) identifikēšanai. Mūsdienās daudzi antivīrusi savās datubāzēs iekļauj arī reklāmas programmatūru un citas potenciāli kaitīgās programmas. Līdz ar to, izmantojot šādus antivīrusus, zūd nepieciešamība noslogot datoru ar papildu pretspiegošanas programmatūru.

Pretsurogātpasta aizsardzība

Lai gan daudziem interneta lietotājiem surogātpasts vēl arvien asociējas ar kaitinošiem reklāmas sūtījumiem, tomēr tas nav nemaz tik „nevainīgs”. Jaunākie dati liecina, ka liela daļa surogātpasta sūtījumu mūsdienās ir ar izteikti krimināli – tajos ir kaitīgas programmas vai saites uz tām, tās aicina ierakstīt savus datus krāpnieku ierīkotās viltus vietnēs utt. Tāpēc pretsurogātpasta programmas tiem lietotājiem, kuri izmanto e-pasta programmas, ir kļuvušas tikpat obligātas kā antivīruss.

Pretsuregātpasta programma veic e-pasta vēstuļu dažādu elementu pārbaudi, lai ar dažādu metožu (signatūras, melnie un baltie saraksti, lingvistiskā analīze, grafiskā analīze u. c.) palīdzību atsijātu nevēlamos sūtījumus.

Privātuma aizsardzība

Viens no izplatītākajiem kibernetiskajiem draudiem internetā pašlaik ir datorkrāpniecība (*phishing*), kad ar īpaši sagatavotu e-pasta sūtījumu palīdzību interneta lietotāji tiek ievilināti krāpnieku interneta vietnēs, piemēram, viltotās tiešsaistes banku lapās. Ar īpašu programmu (*anti-phishing*) palīdzību iespējams identificēt šādas krāpnieku lapas, kā arī nepieļaut kritiskas informācijas noplūdi.

Vecāku kontrole

Vecāku kontroles aizsardzības programmu galvenais uzdevums ir bērnu aizsardzība no nevēlamas informācijas internetā. Ņemot vērā atjaunināmās datu bāzēs, kā arī interneta lapu satura analīzes, tās darbojas kā „cenzors” starp internetu un pārlūkprogrammu, aizliedzot nevēlamo lapu apskati.

Drošības pasākumi

Viena no galvenajām drošības problēmām ar *Windows* operētājsistēmu aprīkoti mājas datoriem ir faktā, ka pēc operētājsistēmas uzstādīšanas lietotājam ir administratora tiesības. Diemžēl tādas pašas tiesības iegūst arī kaitīgās programmas un uzbrucēji. Tāpēc viens no drošības pasākumiem būtu parūpēšanās par lietotāja tiesību ierobežošanu tur, kur tas iespējams. *Windows* datoru, kurā lietotājs strādā ar ierobežotām tiesībām, būtiska kaitīgo programmu daļa nemaz nespēj inficēt!

Ļoti daudzas mūsdienu kaitīgās programmas izmanto programmatūras ievainojamības, kas ļauj inficēt datoru. Tas var notikt pat apmeklējot par uzticamām uzskatāmas interneta vietnes. Tāpēc obligāts drošības pasākums ir operētājsistēmas un citas programmatūras automātisko atjaunināšanas funkciju izmantošana.

Protams, ka drošības pasākumu sarakstu varētu turpināt, tomēr tie būs pa spēkam tikai pieredzējušiem lietotājiem vai speciālistiem. Internetā ir atrodams ļoti daudz resursu ar detalizētām instrukcijām, piemēram, kā padarīt *Windows* operētājsistēmu drošāku.

Ieteikumi

Viens no uzdevumiem, ar ko bieži jāsastopas mājas datoru lietotājiem, ir aizsardzības programmatūras izvēle. Produktu klāsts ir milzīgs, sākot no atsevišķiem antivīrusiem, ugunsmūriem, pretspiegošana programmām u.c. līdz integrētām programmatūras paketēm.

Lai vienkāršotu izvēli un izvairītos no kļūdām, interneta lietotājam ar mazu vai vidēju pieredzi un zināšanu līmeni būtu ļoti ieteicams pievērst uzmanību integrētām aizsardzības paketēm. Šādiem risinājumiem, kas nosaukumā parasti iekļauj vārdus „*Internet Security*”, ir daudz būtisku priekšrocību – aizsardzības komponentes ir salāgotas un nekonfliktē savstarpēji, kopsummā tiek patērēts mazāk datora resursu, aizsardzība ir vadāma caur vienotu interfeisu un, kas pats

būtiskākais, dators iegūst gatavu aizsardzības sistēmu pret visiem izplatītākajiem apdraudējumu veidiem.

Izvēlē starp dažādu ražotāju risinājumiem var vadīties pēc speciālistu ieteikumiem vai novērtējumiem un testiem IT izdevumos. Galvenais, kas jāatceras – nevajadzētu izvēlēties, ņemot vērā tikai vienu avotu.

Ne mazāk būtiski par drošības programmatūras izvēli ir operētājsistēmas iestatījumi un programmatūras atjaunināšana.

Informāciju sagatavoja Valdis Šķesters,

"Kaspersky Lab" pārstāvis Latvijā.