Асновы бяспекі ў Інтэрнэце

Паролі

Паролі з'яўляюцца асновай кожнай палітыкі бяспекі, звычайна пароль – гэта адзінае, што адрознівае сапраўднага карыстальніка ад астатніх. Ён дзейнічае як пашпарт і служыць для таго, каб карыстальнік пераканаў сістэму ў тым, што ён сапраўды той, за каго сябе выдае. Калі пароль быў абраны няўдала, не абавязкова валодаць складанай тэхнікай, каб, **выдаючы сябе за сапраўднага карыстальніка,** увайсці ў сістэму.

Было апублікавана мноства розных даследаванняў на тэму "Найчасцей ужываныя паролі", і бальшыня гэтых працаў у дзесятцы найчасцейшых называе наступныя:

- 123456
- password
- jesus
- love
- dragon
- qwerty
- monkey
- freedom
- iloveyou
- і да т.п.

У аўтаматызаваных атаках гэтыя паролі выпрабоўваюцца у першую чаргу, іх ні ў якім разе не варта выкарыстоўваць. Аўтаматызаваныя атакі часта могуць уводзіць у сістэму некалькі тысяч варыянтаў пароляў за хвіліну і здольныя выпрабоўваць вялізную колькасць пароляў, захаваных у **слоўніках розных моваў**. Базы дадзеных словаў і самых часта ўжываных пароляў можна без праблем знайсці ў Інтэрнэце і аўтаматызавана іх выпрабаваць. Зламысныя праграмы ўлічваюць разнастайныя камбінацыі словаў і іх **простыя варыяцыі** (слова, напісанае ззаду наперад, і г.д.), а таксама выпрабоўваюць паролі, якія складаюцца з вядомай інфармацыі пра карыстальніка (імя, прозвішча, адрас электроннай пошты і да т.п.).

Падбіраючы пароль, варта прытрымлівацца прынамсі базавых правілаў добрага пароля, дзякуючы якім вы зможаце істотна знізіць верагоднасць аўтаматызаванага або мэтанакіраванага раскрыцця вашага пароля:

1. Поўная **адсутнасць пароля** раўняецца адкрытай дарозе ў нашую сістэму. На такія рахункі звычайна нападаюць у першую чаргу.
2. Эфектыўнасць пароля, тоеснага з імем карыстальніка, такая ж, як і пры адсутнасць пароля. Слоўнікавы метад улічвае і гэты варыянт.

Такія паролі правяраюцца **ў першую чаргу**. Гэтаксама няварта выкарыстоўваць у якасці пароля ўласны адрас электроннай пошты і іншыя лёгкадаступныя дадзеныя.

3. Трывіяльныя паролі тыпу ааа, abc, 12345, qwert і г.д. таксама цалкам бессэнсоўныя. Іх вельмі проста **раскрыць**, а пры вялікай колькасці карыстальнікаў вельмі лёгка знайсці таго, хто выкарыстоўвае такі пароль.

4. Любое слова, якое прысутнічае ў **слоўніку**, таксама вельмі няўдалы выбар. Зважаючы на тое, што выкарыстоўваюцца вельмі вялікія слоўнікі, нельга спадзявацца нават на словы абмежаванага ўжытку.
5. Часцей за ўсё для слоўнікавых атак выкарыстоўваюцца слоўнікі некалькіх моваў. Таму нават выкарыстанне **замежных словаў** не дае гарантыі бяспекі.
6. Лёгкадаступныя дадзеныя, такія як нумар тэлефона, дата нараджэння, імя жонкі ці шэфа для пароля не падыходзяць.
Пры мэтанакіраванай атацы іх вельмі проста знайсці і выпрабаваць.
7. Зваротны парадак, злучэнне або простыя **варыяцыі словаў** для сучаснай слоўнікавай праграмы не ўяўляюць ніякай перашкоды. Такія паролі, як uoyevoli, mar1a, qwer123 не з'яўляюцца бяспечнымі.
8. Варта скласці пароль з малых і вялікіх літар і дапоўніць яго спецыяльнымі знакамі, напрыклад: @#$%^*/-} і інш.
9. Пароль, які вы недзе запісалі, не з'яўляецца бяспечным. Ніколі нельга быць упэўненым у тым, што яго ніхто не прачытаў. Вядомыя, напрыклад, выпадкі людзей, якія напісалі PIN-код да сваёй банкаўскай карткі фламастэрам на самой картцы, каб не забыцца. Гэта тое ж самае, як калі б у вас наогул не было пароля.
10. Нават вельмі добры пароль бессэнсоўны, калі яго ведае хто-небудзь, акрамя карыстальніка, якому ён належыць.

Каб запомніць свой пароль, можна выкарыстаць якую-небудзь гульню словаў і з кожнага слова ўзяць, напрыклад, першую літару, а вынік дапоўніць спецыяльнымі знакамі. Напрыклад:

I was father all my life
have no children have no wife.

IWFAML@hnchnw

Гэта добры пароль, які нікому не ўдасца раскрыць, а вы пры гэтым яго не забудзеце. Але гэты пароль ужо ні ў якім разе не выкарыстоўвайце! Гэты дакумент дакладна прачыталі не толькі вы.

Бяспечны кампутар

Каб быць упэўненым у тым, што вашыя дадзеныя і паролі нікому не стануць вядомымі, трэба забяспечыць і ваш кампутар. Ва ўзломшчыка ёсць некалькі магчымасцяў атрымаць доступ да яго зместу або да таго, што вы пішаце на клавіятуры. Існуюць праграмныя інструменты, якія сочаць за карыстальнікам, і пасля таго, як ён увёў пароль, **адсылаюць яго на спецыялізаваны сервер**. Гаворка ў такім выпадку можа ісці як пра дзяржаўныя

праграмы шпіянажу, так і пра звычайныя **кампутарныя вірусы**. Сучасныя вірусы якраз спецыялізуюцца на атрыманні пароляў не толькі ад банкаўскіх рахункаў, але і ад іншых сістэм, якія могуць трапіць у рукі ўзломшчыка.

Яшчэ адной магчымасцю з'яўляюцца праграмы-кілогеры (keylogger) – малыя прыстасаванні, якія падключаюцца паміж клавіятурай і кампутарам або наўпрост інтэгруюцца ў клавіятуру. Выявіць іх часта бывае вельмі праблематычна, а яны ціха запісваюць усё, што карыстальнік на кампутары набірае, і адсылаюць гэтыя дадзеныя свайму першапачатковаму ўласніку. На жаль, такія прыстасаванні можна вельмі танна купіць у Інтэрнэце, а іх падключэнне –пытанне некалькіх секунд.

Яшчэ адным часта злоўжываным прыстасаваннем з'яўляецца вэб-камера. З дапамогай праграмнага забеспячэння яе можна на адлегласці **ўключыць і сачыць за карыстальнікам**. Сёння камера ёсць амаль у кожным ноўтбуку, яна часта прысутнічае ў настольных кампутарах дома і ў інтэрнэт-кавярнях. Бальшыня камер абсталяваная светлавым дыёдам, які паказвае працу. Аднак існуюць спосабы, як уключыць камеру без запалення гэтай лямпачкі. Таму ў часе, калі камера не выкарыстоўваецца, яе рэкамендуецца закрываць або адлучаць.

Асновай аховы ад падобных відаў атак павінна быць **актуалізацыя** аперацыйнай сістэмы і ўсіх прыкладных праграм (перадусім вэб-аглядальніка), актуалізацыя **антывіруснай праграмы** і ўключаны **міжсеткавы экран**. Актуалізацыя сістэмы і прыкладных праграм выпраўляе прабелы ў бяспецы, праз якія зламыснікі заносяць у кампутар свае падступныя праграмы. Калі гаворка ідзе пра вядомы кампутарны вірус, яго дапаможа ідэнтыфікаваць антывіруснае праграмнае забеспячэнне. Супраць дыстанцыйнага злоўжывання сеткавым падключэннем дапаможа якасны міжсеткавы экран, які працуе як фільтр і не прапускае непажаданай для карыстальніка камунікацыі, якая б магла выпрабоўваць розныя тыпы атак на кампутар звонку.

З прыведзенай інфармацыі вынікае, што выкарыстоўваць чужы кампутар (напрыклад, у інтэрнэт-кавярні) для ажыццяўлення аперацый, якія вымагаюць бяспеку, заўсёды рызыкоўна. Заўсёды, калі гэта магчыма, варта выкарыстоўваць уласны кампутар, рэгулярна яго правяраць як з выкарыстаннем праграмных інструментаў, так і з тэхнічнага боку. У выпадку любой анамаліі кансультуйцеся з дасведчаным тэхнікам.

Як бяспечна працаваць на чужым кампутары

Існуюць сітуацыі, калі ў нас проста няма іншай магчымасці і мы мусім выкарыстаць чужы кампутар або кампутар у інтэрнэт-кавярні. У такім выпадку мы ніколі не можам быць упэўненыя, што сістэма не заражаная вірусам або іншымі праграмамі, якія адсочваюць дзеянні карыстальніка. Гэта можа быць наўмысна ўсталяваная прыкладная праграма або проста вірус, які трапіў у кампутар, таму што на ім працавала зашмат розных карыстальнікаў (інтэрнэт-кавярня), а забеспячэнне было недастатковым.

У такой сітуацыі дапамагчы можа толькі адно – запусціць на кампутары ўласную аперацыйную сістэму, якая не мае нічога агульнага з сістэмай, усталяванай на кампутары, і не змяшчае яе падступныя коды. Натуральна, што не ўсюды такая аперацыя магчымая, да таго ж, яна можа выглядаць падазрона сама па сабе, але калі гэта магчыма, варта ўзважыць гэты варыянт. Сістэму, запушчаную з вашага носьбіта, вы можаце цалкам кантраляваць, можаце ажыццявіць у ёй неабходныя аперацыі, а потым зноў вярнуць усё ў першапачатковы стан.

Такіх аперацыйных праграм існуе цэлы шэраг, звычайна яны базуюцца на Linux. Мы рэкамендуем выпрабаваць дыстрыбутыў Linux Slax (www.slax.org), які можна запісаць на CD/DVD або ўсталяваць на флэш-дыск/знешні цвёрды дыск. Потым дастаткова ўставіць/падлучыць носьбіт да кампутара, перазагрузіць і на старце абраць запуск сістэмы з дадзенага носьбіта. Ён запусціць паўнавартасную аперацыйную праграму, якая працуе з вашага носьбіта і не будзе звязаная з дыскам у кампутары. Акрамя таго, што гэтая сістэма не можа змяшчаць ніякіх вірусаў і шкоднага праграмнага забеспячэння, вы не пакінеце ў базавай аперацыйнай сістэме ніякіх слядоў сваёй працы. Як толькі вы скончыце працу, выключыце кампутар, адлучыце носьбіт, а пасля ўключэння зноў запусціце кампутар ў стандартным рэжыме.

Згаданы Slax прапануе асноўны камплект прыкладных праграм, у які ўваходзіць вэб-аглядальнік, просты офісны пакет, мультымедыйны прайгравальнік, кампрэсійныя утыліты, праграмы для спампоўвання і інш. На хатняй старонцы праекту можна дадаткова спампаваць некалькі сотняў іншых праграмаў, якія вы можаце ўсталяваць часова падчас працы Slax або запісаць іх наўпрост на флэш-дыск, дзе яны ў вас захаваюцца.

На флэш-дыск можна таксама дадаць прыкладныя праграмы, патрэбныя для шыфравання з дапамогай ключа GPG, шыфравання дадзеных на дыску (TrueCrypt) ці для падлучэння да сеткі TOR. Гэтыя прыкладныя праграмы будуць апісаныя ў гэтым тэксце ніжэй. Звярніце ўвагу, што ў сістэму Slax немагчыма ўсталяваць праграмы, прызначаныя для Windows. Праграмы вы знойдзеце на адрасе www.slax.org.

Шыфраванне перадаванай інфармацыі

У звычайных умовах значная частка перадачы дадзеных у Інтэрнэце адбываецца без ніякай шыфроўкі і праходзіць праз мноства вузлоў па ўсім свеце. Ва ўсіх гэтых пунктах можна сачыць за камунікацыяй і захоўваць цікавую ці канфідэнцыйную інфармацыю. Такім чынам магчыма не толькі атрымаць розныя імёны карыстальнікаў і паролі, а таксама перадаваную інфармацыю цалкам, такую як электронныя паведамленні, розныя файлы, інфармацыю, перадаваную праз праграмы імгненнага абмену паведамленнямі (Live Messenger, ICQ і іншыя).

Таму мае сэнс загадзя праверыць, ці шыфруецца камунікацыя. Звычайна гэта можна высветліць у даведцы канкрэтных сеткавых праграм, такую інфармацыю можна знайсці і

ў Інтэрнэце. У выпадку прагляду вэб-сайтаў сітуацыя адносна простая: некаторыя сайты дазваляюць уключыць шыфраванне. Тое, шыфруецеся вы ці не, можна даведацца па вэб-адрасе. Калі ён пачынаецца з http://, шыфраванне не ўключанае. Калі вы зменіце адрас на https:// ("s" значыць “secure”), шыфраванне актывуецца. Яно пазначаецца іконкай малага жоўтага замка ля адрасу.

Аднак не кожная служба прапануе шыфраваны варыянт. Напрыклад, службы Google дазваляюць уключыць шыфраванне, вы можаце чытаць пошту і карыстацца пошукам у рэжыме шыфравання. Перадаваныя дадзеныя, такім чынам, будуць даступныя толькі вам і Google. Некаторыя службы (напрыклад, банкі і іншыя) шыфраванне нават вымагаюць, і без яго вы не атрымаеце доступ ні да якой інфармацыі.

Калі шыфраванне ўжо ўключанае, варта праверыць і таго, хто выдаў “сертыфікат”. Гаворка ідзе пра арганізацыю, якая правярае, ці сапраўды старонкі, якія праглядаюцца, належаць таму, каму павінны належаць. Калі праверка не адбылася, за ўласніка сайта можа сябе выдаваць абсалютна хто заўгодна. Такім чынам, калі вы шыфруецеся, клікніце на іконку замка і паглядзіце, хто выдаў канкрэтны сертыфікат. Да самых вядомых і надзейных сервісаў сертыфікатаў належаць, напрыклад, Thawte і VeriSign. Калі старонка прадставіць вам іхні сертыфікат, вы можаце быць упэўненыя, што дакладна ўводзіце свой пароль на сапраўднай старонцы, а не на фальшывай імітацыі, якая такім чынам завалодае вашым паролем.

Шыфраванне дадзеных на дыску

Вялікая колькасць карыстальнікаў у наш час карыстаецца ноўтбукамі або знешнімі цвёрдымі дыскамі з каштоўнымі дадзенымі. У выпадку крадзяжу такога прыстасавання пагражае і крадзеж сакрэтных дадзеных, якія звычайна больш каштоўныя, чым само прыстасаванне. Адзінай аховай з’яўляецца шыфраванне дадзеных на дыску. Існуюць інструменты, інтэграваныя наўпрост у аперацыйныя сістэмы (Windows, Mac OS X і Linux), а таксама знешнія. Перавагай інструментаў трэцяга боку ёсць іхняя універсальнасць: іх можна выкарыстоўваць адначасова ў розных асяродках і аперацыйных сістэмах.

Сярод такіх інструментаў можна парэкамендаваць праверaны інструмент TrueCrypt. Ён даступны бясплатна, і яго можна спампаваць з сайту www.truecrypt.org. Дадзены інструмент вы павінны ўсталяваць у сваёй аперацыйнай сістэме, і ён прапануе вам стварэнне новага шыфраванага дыска. Можна зашыфраваць увесь дыск (уключна з аперацыйнай сістэмай) або стварыць на знешнім прыстасаванні толькі невялікую зашыфраваную зону. Потым для атрымання доступу да сваіх дадзеных вам трэба будзе ўводзіць пароль. Бяспечнасць такога рашэння залежыць ад бяспечнасці абранага паролю.

На выпадак больш сур’ёзных праблемаў TrueCrypt дазваляе ствараць так званыя схаваныя зоны. Гэта зашыфраваныя дыскі ўнутры зашыфраваных дыскаў. У такім выпадку да аднаго сховішча існуе некалькі пароляў. Калі вы, напрыклад, будзеце вымушаныя

выдаць пароль, вы можаце паведаміць толькі адзін з іх. Зламыснік у гэтым выпадку атрымае доступ да фальшывай інфармацыі, якая ўсё ж мусіць быць настолькі праўдападобнай, каб задаволіць яго і прымусіць перастаць дапытвацца пра іншыя паролі. Унутры зоны існуе яшчэ адзін схаваны дыск, доступ да якога вы атрымаеце толькі пасля ўводу другога паролю. Калі вы гэтага паролю не ведаеце, вы не зможаце не толькі атрымаць інфармацыю, але і даведацца, што яна існуе.

Бяспечнасць TrueCrypt была пацверджаная шматлікімі экспертамі і тэстамі, на гэтае праграмнае забеспячэнне можна спадзявацца на сто адсоткаў і даверыць яму свае дадзеныя. Аднак не забывайцеся пра якасны пароль.

Бяспечная электронная пошта

Электронная пошта з'яўляецца службай, якая часта бывае аб'ектам атак спаму або мэтанакіраваных падманных паведамленняў. Гаворка ідзе пра адну з найстарэйшых службаў у Інтэрнэце, і менавіта таму яна не змяшчае ніякіх механізмаў бяспекі. Таму вельмі проста сфальшаваць адрас адпраўшчыка, змяніць любое паведамленне, якое перамяшчаецца ў Інтэрнэце, і гэтак далей. Праз лічбавую сутнасць прынцыпу электроннай пошты такія змены практычна немагчыма выявіць, а зламыснік можа такім чынам вельмі лёгка маніпуляваць ахвярай.

Адзінай аховай зноў з'яўляецца шыфраванне або электронны подпіс. Ён дазваляе атрымальніку праверыць, што паведамленне было дасланае сапраўдным адпраўшчыкам і што яно не было ніякім чынам зменена. Подпіс трывала звязаны са зместам паведамлення, яго немагчыма перанесці на іншае паведамленне, а таксама немагчыма змяніць ніводнай літары ў паведамленні без таго, каб гэта выявіла праграмнае забеспячэнне атрымальніка.

Існуе некалькі розных магчымасцяў электроннага подпісу і шыфравання электронных паведамленняў, самымі папулярнымі сярод звычайных карыстальнікаў з'яўляюцца GPG або GnuPG. Гэта варыянт, сумяшчальны з PGP, які дазваляе даволі простым шляхам стварыць уласны сертыфікат подпісу, атрымліваць і адміністраваць сертыфікаты астатніх карыстальнікаў і камунікаваць з паасобнымі праграмамі.

Працэс усталявання ў Windows просты. Спампуйце і ўсталюйце GPG4Win (http://www.gpg4win.org/), які з'яўляецца наборам прыкладных праграм, неабходных для працы з GPG. З дапамогай праграмы GPA стварыце ўласны сертыфікат і атрымайце сертыфікат другога боку. Каб любы карыстальнік мог атрымаць ваш сертыфікат, правядзіце яго экспарт на сервер з ключамі. У выніку гэтага любы карыстальнік зможа пераканацца, што вашыя паведамленні падпісаныя сапраўдным подпісам, які належыць вам. У той жа час дадзеныя, якія трапяць на сервер і да іншых карыстальнікаў, немагчыма выкарыстаць для подпісу вашым імем.

Калі вы ўсталявалі і падрыхтавалі ядро GPG адпаведным чынам, выкарыстайце паштовы

кліент Thunderbird, у які даўсталюйце пашырэнне Enigmail. Яно аўтаматычна злучыцца з вашым GPG, і вы можаце адразу ж пачынаць шыфраваць ці падпісвацца. Для подпісу вам патрэбны толькі ўласны ключ, які вы генеравалі, для шыфравання вам спатрэбяцца і ключы карыстальнікаў, з якімі вы будзеце кантактаваць. Калі і ў астатніх карыстальнікаў ёсць GPG, яны могуць прымаць вашыя шыфраваныя і/ці падпісаныя паведамленні. Такім чынам вы можаце перадаваць нават строга сакрэтную інфармацыю, доступ да якой атрымае толькі вызначаны вамі карыстальнік.

Ананімны прагляд Інтэрнэту

Часам бывае неабходна праглядаць вэб-сайт так, каб яго ўладальнік не бачыў, хто яго праглядае. Кожны адміністратар сайта можа бачыць розную інфармацыю пра наведвальнікаў, напрыклад, IP-адрас карыстальніка, прыблізнае месцазнаходжанне карыстальніка (часам на дзіва дакладнае), усталяванае праграмнае забеспячэнне, версію аперацыйнай сістэмы і іншую інфармацыю. Таксама можна даведацца, якія старонкі карыстальнік наведаў раней і г.д. Гэта звесткі, якія б мы часам хацелі схаваць.

Адным са спосабаў з'яўляецца выкарыстанне так званых ананімайзераў. Гэта вэб-старонкі, якія ўваходзяць на патрэбны сайт "за нас" і робяцца нашымі пасярэднікамі. У такім выпадку ўладальнік вэб-сайта бачыць інфармацыю пра дадзены ананімайзер, а не пра нас. У Інтэрнэце існуюць сотні ананімайзераў, паспрабаваць можна, напрыклад, Anonymouse.org або ўвесці ў Google ключавое слова "anonymizer" і знайсці іншы. На сайце ананімайзера дастаткова ўвесці адрас патрэбнага кампутара ў адпаведную калонку і праглядаць, як звычайна. Пры ананімным праглядзе адрас у браўзеры заўсёды павінен пачынацца з адрасу ананімайзера.

Другім і значна больш складаным варыянтам з'яўляецца выкарыстанне сеткі TOR. Гэта сетка сотняў сервераў па ўсім свеце, праз якія вы можаце накіроўваць усю сваю камунікацыю з вонкавым светам. Уся камунікацыя некалькі разоў шыфруецца, таму нават самі гэтыя серверы не ведаюць, хто з кім насамрэч камунікуе. Усё абсалютна засакрэчана.

Для выкарыстання сеткі TOR вы павінны ўжываць вэб-аглядальнік Firefox і ўсталяваць толькі праграму Vidalia. Яе можна знайсці на адрасе https://www.torproject.org/projects/vidalia. Пасля ўсталявання праграмы ў вашай сістэме побач з гадзіннікам дадасца іконка цыбуліны. Калі вы на яе клікнеце, з'явіцца просты інтэрфейс кіравання. У ім актывуйце падключэнне да сеткі TOR. Потым запусціце Firefox, у якім таксама дадасца новая кнопка. З яе дапамогай вы зможаце лёгка ўключаць і выключаць выкарыстанне сеткі TOR.

Праверка функцыі простая: наведайце сайт www.whatismyip.com і паглядзіце, які IP-адрас у вашага кампутара. Потым уключыце TOR і зайдзіце на сайт яшчэ раз. Ваш IP-адрас павінен адрозніваца. Калі вы праз нейкі час зноў зойдзеце на сайт, ваш IP-адрас зноў будзе іншым. Гэта адбываецца таму, што TOR выкарыстоўвае шмат розных сервераў

па ўсім свеце і пастаянна (кожныя некалькі хвілін) змяняе шлях, па якім праходзяць вашыя дадзеныя. Таму выглядае, што ваш кампутар знаходзіцца то ў Нідэрландах, то ў Францыі, то ў Канадзе. Рэальнае месцазнаходжанне пры ўключаным TOR ніхто не ўбачыць.

Гэты варыянт вельмі бяспечны, існуюць тэарэтычныя магчымасці атакі на сетку TOR, але на практыцы ніводная з іх не была паспяхова выпрабаваная. Недахопам гэтага варыянту з'яўляецца тое, што праца праз TOR значна запаволеная ў параўнанні са звычайным шляхам. Мы ні ў якім разе не рэкамендуем спампоўваць праз TOR вялікія аб'ёмы дадзеных. Гэта сістэма прызначаная для прагляду вэб-сайтаў. Аднак звярніце ўвагу на тое, што вы можаце выдаць сябе тым, што ўведзяце на нейкім вэб-сайце свае асабістыя дадзеныя. Напрыклад, пры ўваходзе на Facebook будзе выглядаць, што ваш кампутар знаходзіцца ў Егіпце, але дзякуючы вашаму ўваходу Facebook будзе ведаць, што гэта вы.

Рызыкоўныя праграмы

Выкарыстанне некаторых праграмаў нясе большую небяспеку, чым звычайна. Прычынай гэтага можа быць тое, што яны не надта зважаюць на бяспечнасць або змяшчаюць вядомыя памылкі ў бяспецы. Такіх праграмаў лепш пазбягаць, таму што яны дарэмна ставяць вас у небяспечную сітуацыю. Ніжэй прадстаўлена некалькі такіх праграмаў.

Internet Explorer ужо доўгі час належыць да вельмі праблематычных праграмаў, таму што змяшчае шмат сур'ёзных недахопаў у бяспецы, якія да таго ж на працягу месяцаў застаюцца незалатанымі. Вялікая колькасць зламыснікаў накіроўвае сваю ўвагу менавіта на гэтыя праблемы, а ў выпадку ўдалага злоўжыцця прабелу ў бяспецы часта дастаткова толькі наведаць заражаны вэб-сайт.
Рашэнне: выкарыстоўвайце іншы вэб-аглядальнік, напрыклад, Firefox або Chrome.

Flash Player уваходзіць у большасць кампутараў, таму што карыстальнікі ўжываюць яго для інтэрнэт-гульняў і прагляду відэа з YouTube і іншых сервераў. На жаль, і Flash Player вядомы сваёй "дзіравасцю". На жаль, вартай альтэрнатывы для яго не існуе.
Рашэнне: правярайце актуальнасць свайго Flash Playeru (http://tiny.cc/tn0u4) і выкарыстоўвайце пашырэнне FlashBlock, якое дазваляе запускаць Flash толькі на пэўных вэб-сайтах.

Skype – гэта вельмі пашыраная камунікацыйная праграма для перадачы відэа і голасу ў Інтэрнэце. Яго стваральнікі сцвярджаюць, што гэтая праграма выкарыстоўвае моцнае шыфраванне, гэта пацвярджаюць і эксперты па бяспецы. Аднак некаторыя краіны ўжо пацвердзілі, што заключылі з уладальнікам сеткі Skype дамову аб прадстаўленні доступу да пэўных размоваў. Да гэтых краінаў належаць Кітай, ЗША і Аўстрыя. Аднак не выключана (а нават вельмі верагодна), што іх значна больш.
Рашэнне: не перадавайце праз Skype канфідэнцыйную інфармацыю, выкарыстайце для гэтага альтэрнатыву, напрыклад, GTalk.

Adobe Reader – гэта папулярная праграма для чытання файлаў PDF. На жаль, яна таксама з'яўляецца прычынай шматлікіх праблемаў з бяспекай, перадусім таму, што здольная інтэграваць у вэб-аглядальнік, а небяспечны PDF, які выкарыстоўвае прагал у бяспецы, можа быць часткай вэб-сайта.
Рашэнне: усталяваць альтэрнатыву, напрыклад, Evince, Foxit Reader або PDF-XChange Viever.

У любым выпадку павінна дзейнічаць правіла, што ўсталёўваць можна толькі праверaныя праграмы, якія вы будзеце рэгулярна актуалізаваць.

Фарматы, якія выкарыстоўваюцца для абмену дадзенымі

Вельмі часта карыстальнікам трэба перадаваць у Інтэрнэце канфідэнцыйныя дакументы, сапраўдны аўтар якіх павінен быць засакрэчаны. У такім выпадку ключавым з'яўляецца выбар фармату, таму што некаторыя фарматы перадаюць і схаваную інфармацыю, такую як імя аўтара, наладкі яго кампутара і г.д. Калі вы хочаце засакрэціць гэтыя звесткі, варта абраць фармат, які іх не перадае. Вельмі няўдалым выбарам у такіх выпадках з'яўляюцца фарматы **.doc, .xls і да т.п.**, якія, на жаль, шырока распаўсюджаныя. Яны захоўваюць у сабе шмат падрабязнасцяў пра карыстальніка. Да таго ж, у файлах часта змяшчаюцца і **фрагменты зусім іншых дакументаў**, над якімі карыстальнік працаваў раней! Гэта тлумачыцца тым, што Word намагаецца паскорыць сваю працу і захоўвае ў дакумент частку сваёй працоўнай памяці ў тым выглядзе, у якім яна на дадзены момант ёсць. На жаль, у гэтай памяці звычайна ляжаць і вялікія ўрыўкі ўжо зачыненых дакументаў.

Калі вы хочаце быць упэўненыя, што такія звесткі не трапяць у захаваны файл, заўсёды высылайце канфідэнцыйныя дадзеныя ў **файлах PDF**. Самым простым шляхам да іх стварэння з'яўляецца ўсталяванне так званай віртуальнай друкаркі, якую прапануе, напрыклад, праграма doPDF. Пасля ўсталявання ў вашай сістэме з'явіцца яшчэ адна друкарка. Калі вы "надрукуеце" на ёй любы дакумент, замест сапраўднай раздрукоўкі адчыніцца згаданая праграма, якая спытае вас, як і дзе вы хочаце стварыць PDF. Пры гэтым спосабе камунікацыі (з праграмы, якая друкуе на друкарцы) перадаюцца сапраўды толькі выявы – то бок тое, што б з'явілася на паперы. Ніякія іншыя дадзеныя ў PDF не перадаюцца.