Bulgarian Security Info

Българското списание за сигурност.
Брой 2 - 2008 година

www.virusinfo-bg.org

Bulgarian Security Research Center

LOD TS, Bulgarian Portal Network

Bulgarian Security Info

- Седмично списание за компютърна сигурност.
- Съдържание:
  - Защита чрез Firewall в Internet пространството за една организация 3-5 стр.
  - Съвременните заплахи за IT сектора 6-9 стр.
  - Обща информация за вирусите част 2-ра 10-14 стр.

Защита чрез Firewall в Internet пространството за една организация

- 1-Какво представлява Firewall

Firewall – това е система или група от системи, чрез която се осъществява защитната политика между мрежата на организацията и Internet. Firewall определя, кои вътрешни сървизи могат да бъдат достъпни отвън, кои външнипотребители могат и кои не,за да имат достъп до определени вътрешни сървизи, както и кои външни (Internet) сервизи са достъпни за потребителите на частната мрежа. Необходимо е Firewall да бъде така изграден, че да осигури само, наоторизирания трафик да премине през него, а от своя страна и самият Firewall да бъде осигурен срещу неправомерно проникване. За съжаление Firewall не могат да бъдат много ефективни след като, атакуващите вече веднъж са проникнали в него.Важно е да се отбележи, че Firewall не е само маршрутизатор, bastion host или комбинация от устройства, които осигуряват защита на мрежата. Firewall е често цялостна защитна политика, която създава област, защитена от атаки. При определянето на защитната политика е необходимо да се публикуват правила за защита, с които се информират потребителите за техните отговорности; определят се корпоративни правила за достъп до мрежата; достъпа до Internet сервизите и пр.Всички точки за потенциална атака на мрежата трябва да бъдат защитени с едно и също ниво на мрежова защита.

Защита чрез Firewall в Internet пространството за една организация

- 2-Ползата от Firewall

Internet Firewall управлява достъпа между Internet и частната мрежа . Без Firewall всяка една система от частната мрежа е изложена на атаки от другите хостове в Internet. Това означава ,че сигурността на частната мрежа зависи от това ,до каква степен са защитени отделните хостове в нея, а сигурността на мрежата е точно толкова защитена ,колкото и най-слабо защитеният в нея хост. Internet Firewall позволява на мрежовия администратор да дефинира централизирана "choke point", която държи неоторизираните клиенти извън защитената мрежа. Internet Firewall опростява управлението на сигурността в мрежата с помощта на различни средства за мониторинг и средства за следене. Необходимо е администраторът да следи стриктно всички log files за трафика през Firewall и да реагира на всички алармиращи събития.Internet Firewall е чудесно средство за следене на трафика и използването на Internet. Това позволявана мрежовия администратор да оправдае средствата изразходвани от осъществяването на връзката с Internet до неговото управление, както и да определи метод за таксуване на отделните отдели в организацията, ако това отговаря на нейния финансов модел.Internet Firewall не може да защити мрежата от прехвърлянето на софтуери или файлове, носители на вируси. Поради голямото разнообразие на операционни системи, различни начини за кодиране и компресиране на файлове, не евъзможно да се очаква Internet Firewall да сканира всеки един файл за вируси. С оглед на това е необходимо да бъде инсталиран анти-вирусен софтуер на всеки потребителски компютър. Internet Firewall не може да защити мрежата и от "data-driven" атаки. Те се случват, когато потребител от защитената мрежа получи по електронната поща или копира на пръв поглед безвредни данни или информация и стартира съответното приложение. При такива ситуации е възможно да се предизвика промяна на файловете, касаещи сигурността на мрежата и по този начин осигуряват лесен достъп до системата на неоторизирани потребители.

Защита чрез Firewall в Internet пространството за една организация

- 3-Слабите страни на Firewall

Firewall предпазва от извличането на поверителна информация за мрежовата връзка. Обаче същите данни могат да се копират на дискета, магнитни носители или върху хартия. Ако атакуващият е преминал защитната стена, то тя става безполезна. Вътрешните потребители могат да увредят харддиска, софтуера или да променят програми без въобще да влизат в контакт със защитната стена. Защитната стена може да контролира много добре трафика през себе си, обаче не може да повлияе върху трафика, който не минава през нея. Технически компетентни потребители или системни администратори си създават една задна вратичка за Интернет, защото се ядосват на прекалените ограничения на защитната стена. Firewall е беззащитна срещу това. Тук вече не става въпрос за технически, а по-скоро за личен проблем. Една защитна стена се планира така, че да предпазва от познатите опасности. Една добра защитна стена може да предпазва от бъдещи опасности, само ако в нея се разрешат строго определени безопасни услуги. Но от конфигурирането не можем да изхождаме, че тя ще ни пази добре. Firewall не може да предпазва мрежата от вируси. Повечето защитни стени проверяват всъщност целия трафик, който минава през тях, за да установят, че данните са безопасни и да им позволят да преминат. Това са на практика само адресите на източника и получателя ,както и номерата на портовете.,не обаче съдържанието на данните. Прагматичното решение на проблема с вирусите са защитни програми на всеки отделен компютър и разясняването на потребителите за опасността от вируси и за подходящите защитни мерки.

Автор:**mihnev_sz**

М. Михнев
e-mail: mihnev_sz@abv.bg
Skype: mihnev_sz

Съвременните заплахи за IT сектора

- През 20 век не можем да говорим за вируси , като имаме в предвид онова им познато име от период на тяхното създаване . В началото на 20 век се появяват и други заплахи за информационната сигурност , които имат свои собствени имена според това какво правят . Появяват се т.н. червеи , троянски коне , шпионски софтуер (spyware) , adware (рекламен софтуер) , hack tools (хакерски устройства) , rootkits и др.
- Докато през 20 век вирусите се разпространяват бавно , дори много бавно , развитието на глобалнана мрежа интернет спомага изключително много за това през 21 век да се появят и другите заплахи .
- Измислянето на имена се е породило в края на 20 и началото на 21 век , като то условно разделя заплахите :
- Вирусите са зараза , която поврежда съществуващи файлове на даден компютър като по този начин прави файла невъзможен за употреба . Вирусите заразяват предимно изпълними файлове (com,exe,scr...) и документи . Името на вирусите идва от билогията , тъй като компютърният вирус действа по подобен начин като биологичния вирус . За да се разпространява , вирусът обикновено се прикачва към края на даден файл и започва да се само репликира единствено и само след като е стартиран на компютъра на жертвата

Съвременните заплахи за IT сектора

- Троянските коне не се саморепликират и обикновено не повреждат други файлове . Тяхното име и предназначение е исторически свързано с извесния Троянски кон от Древно-гръцката митология . Троянските коне са програми , които се представят по един привлекателен начин , но всъщност извършват други действия . Точно както в „Иляда" програма троянец привлича даден потребител , по някакъв начин излъгва потребител да я стартира , в началото тя се представя за нещо добро , но в последствие (попринцип тайно) извършва истинските си действия . Троянски кон може да извършва всичко – примерно да изтегля други заразени файлове , да шпионира , да отваря „вратички" през защитата на потребител , за да бъде потребителската машина контролирана от хакер , може да набира импулсни номера и пр.
- Червеите (worms) се разпространяват по мрежата и/или по email . Те могат да се репликират, но обикновено не заразяват други файлове . Основната им цел е след като пристигнат при даден потребител , червеят да се докосне и до други машини възможно най-бързо с цел претоварване на мрежи и в последствие загиването на мрежата . Червеите могат и да се репликират и локално с цел претоварване на заразената машина . Типичен пример за локано и мрежово претоварване е червеят Brontok .
- Шпионският и рекламен софтуер се използва за шпиониране на действията на потребител и предаване на събраната информация на трети лица , които да я използват в своя полза . Шпионската програма може да събира всякаква информация , а рекламният събира информация с цел последваща реклама
- Rootkits са злото на 21 век . Те предоставят на създадете си неограничен достъп до заразения компютър , но прикривайте своето присъствие . След като биват „заредени" в машината на жертвата те действа в ядрото на операционната система като по този начин се прикриват от обикновените антивирусни програми . Обикновената антивирусна защита е неспособна да види заплаха , още по-малко да се справи с нея .

Съвременните заплахи за IT сектора

- Може би сте забелязали , че при описването на всяка една от заплахите съм използвал думата „обикновено" прекалено често ? Да , така е , но не е случайно . Може би също знаете , че информационните технологии се развиват прекалено бързо ? Е , това важи с двойна сила за зловредния код . Заплахите , които се появиха в глобалната мрежа през 2006 и тези , които се появат и днес са все по-сложни и по-заплетени . Те са комбинация и трудно могат да се нарекат само с едно име . Даден червей не просто пренатоварва мрежата , ами и изтрива файлове . Вирусите не просто повреждат файлове , те ги унищожават напълно без опция за изчистване/поправяне , разлика между троянски кон , който шпионира и обикновен рекламен/шпионски софтуер е много много тънка . Заплахите на 21 век могат да правят всичко . И дори и да сте заразени с троянски кон , то бъдете сигурни , че той ще се опита да вземе ваша информация , ще е зависим от мрежата , ще се опита да изтегли други файлове , които да унищожат операционната ви система , може би ще даде на хакер достъп до машината ви.
- Чудите се за какво му е на някой хакер точни вашите данни , какво правити вие , за да се нуждае от вашата информация ? Най-често потребител е жертва/мулето на друга по-голяма операция . На хакера може да му се достави удоволствие за унищожи компютъра Ви , но вашите ресурси най-често биват използвани за други „благо" . Напоследък е модерно дадена заплаха да служи за примамка и в последствие да се заразите със заплаха , която да даде достъп на хакер до компюта ви . Хакерите използват това си право и употребяват машините ви за да атакуват други компютри , примерно . Конкретен пример – по време на Коледните и Новогодишни празници 2007 г в глобалната мрежа беше пуснат червей Storm/Nuwar , който превръща машината Ви в зомби . Обикновения потребител не може да забележи , че нещо става , но всъщност този червей е успял да превърне близо 700 компютъра от цял свят в зомбита . Хакерите ще използват тези компютри за свои цели , а ресурсите на 700 компютъра са много по-мощна сила от ресурсите на 10-20 , или дори 50 компютъра . Хакерите могат да извършват незаконни действия , като например атаки на големи сайтове/сървъри с цел тяхното пренатоварнане , което води и до тяхното унищожение

Съвременните заплахи за IT сектора

- Друга причина хакер да се нуждае от вашата информация е напълно комерсиална . Все по-популярно е използването на услуги като интернет банкиране и/или пазаруване on-line . Много е удобно , защото спестява изключително много време . Заплаха като троянски кон или rootkit може да предостави кодовете Ви за достъп до банковите Ви сметки и скоро след това да се окажете без пари .
- Типичен пример:
- http://www.standartnews.com/bg/article.php?d=2007-10-17&article=207700
- И има много случаи като този , описан в „Стандарт" , за съжаление в България не се говори толкова много за тях .
- Бъдещето на развитие на заплахите :
- Интернет се разразства с всеки измил ден . По цял свят все повече хора ще се докосват до прелесните , които това уникално явление –Интернет предлага . Модерните заплахи са зависими от интернет , те се раждат в глобалната мрежи , извършват своята мисия за определен период от време и загиват , отново в интернет . Модерните компютри са все по защитени от само себе си , т.е. производителите обикновено ги защитават добре . Днешните заплахи не могат от само себе си да проникнат в даден компютър , затова те използват трикове („търговски" трикове) и докато не се научим да казваме НЕ заплахите винаги ще съществуват .
- ESET – Think Smart !

Автор:**ASpace**

А. Спасов

Обща информация за вирусите част 2-ра

- Успехът на компютрите, компютърните мрежи и Интернет през 90-те години затрудняват още повече усилията за борба с вирусите. Тъй като всички хора се свързват във виртуално общество и започват свободно да обменят файлове и дискети, компютърните вируси започват да се разпространяват в големи мащаби. Синхронизацията на пускане на макро-вируси е съвършена, започвайки с вируса Concept през 1995 г., а стратегията за възпроизвеждане се оказва високоефективна. Макровирусите (т.е. вируси, предавани чрез макроси) заразяват документи на Microsoft Word и може да бъдат предавани и на двете платформи — Macintosh и PC чрез заразени файлове на Word, предавани чрез дискети или по електронна поща.
- Индустрията за антивирусен софтуер и корпоративна Америка започват да губят почва под краката си в усилията си да се предпазят от вирусите на свобода. Компании като Microsoft са объркани от появата на пазар на два търговски компактдиска, заразени с вируса Concept. Стратегиите за защита, знанията и антивирусния софтуер, ако изобщо е имало такива, са още в начален стадий на развитие в много корпоративни среди.
- Към края на 1996 г. макровирусите заемат първо място като най-разпространение вируси на свобода. С внезапното отприщване на вирусите медиите отново откриват, че вирусите са много благодатна тема за новини. Страхът от заразяване с компютърни вируси е посят в сърцето и ума на милиони компютърни потребители по цял свят. Почти всеки познава някой, който е пострадал от компютърен вирус или е чувал за зловредна програма, изтрила всичко на един компютър.
- Последните няколко години на миналото хилядолетие произведоха нови заплахи и за двете платформи Macintosh и PC. През 1998 г. се появи „червеят" Autostart — първият значителен вирус за Macintosh от четири години насам. Потребителите на Интернет започват да се сблъскват с атаки от рода „отказ от услуги", създадени с новите технологии на Java и JavaScript. Червеи като Melissa и Happy99.exe (SKA) получават широко разпространение чрез електронната поща.
- Хилядолетието завършва с твърде голям страх, внушен на средностатистическия компютърен потребител. Толкова много технологии се промениха за толкова кратко време, че хората започнаха да се питат: „Какво в края на краищата, могат да правят компютрите?" Компютрите се превръщат в неоценимо средство за работа на средния домашен или корпоративен потребител. Опасенията от загуба на часове работа или ценни данни е основателен с все по-нарастващата зависимост от компютърните технологии.

Обща информация за вирусите част 2-ра

- **Хронология на компютърните вируси**
- 1970 Първи съобщения за вируси.
- 1986 Brain — първият вирус за PC.
- 1988 Internet Worm.
- 1991 Първи полиморфни вируси.
- 1992 Истерията „Микеланджело".
- 1992 WinVir — първият вирус за Windows.
- 1993 MS-DOS 6 и MSAV.
- 1995 Concept — първият макровирус за Microsoft Word.
- 1996 Първият вирус за Windows 95.
- 1996 Първи макровируси за Microsoft Excel.
- 1997 Първият вирус за Windows NT.
- 1998 Първи макровируси за Microsoft Access.
- 1999 Нова ера за злонамерения софтуер.

Обща информация за вирусите част 2-ра

- **Злонамерен софтуер**
- „Злонамерен софтуер" (malware, от „malicious software"; понякога ще използваме за краткост понятието „малуер" и на български език — бел. прев.) е общо понятие, което обхваща голям диапазон от всякакъв нежелан софтуер — компютърни вируси, атаки от типа „отказ на услуги", „Троянски коне", „червеи" и т. н. Използваната на английски език дума ..malware" произлиза от съчетаването на думите „MALicious" (злобен, злонамерен) и „softWARE" (софтуер). Злонамерен софтуер е всякакъв вид софтуер, създаден с „лоши" намерения. Някои видове злонамерен софтуер като макровируса Concept имат за цел само да се репродуцират, докато други — като Chernobyl (семейство СШ) могат да изтриват съдържанието на цели дискови устройства.
- В дефиницията на злонамерен софтуер понякога попадат и шегобийс-ки програми като Joke.Win.Stupid. Такива шегобийски или „лъжливи" програми обикновено се създават с цел закачка, а не с намерение да навредят. Така нареченият „спам" (spam — широко понятие за нежелани съобщения по електронна поща като обиди, реклами и всякакъв друг вид „електронен болкук" — бел. прев.), например шегаджийски електронни съобщения като PenPal Greetings, не е софтуер и не се включва в официалната дефиниция на злонамерен софтуер. Все пак някои потребители изпадат в паника, щом прочетат в съобщение по електронната поща предупреждение за „изчезване" на компютъра. Когато настъпи паника, потребителят може да изключи неправилно компютъра си и така да повреди файлове, операционната система, а дори и хардуерни компоненти — например дисково устройство. Такива „невинни" измами понякога причиняват много повече щети, например защото информационният отдел в дадена компания трябва да изгуби много време и усилия та предотврати, съхрани и предпази данните от заплаха, която на практика не съществува. „Великденските яйца" и скритите подписи, поставяни понякога от програмистите в техните продукти, не се считат за злонамерен софтуер. Такива елементи понякога се разкриват след натискане на определена клавишна комбинация или настъпване на логически аргумент, например в определен ден от месеца. Истинските „ве-тикденски яйца" са предназначени за забава (без лоши намерения или - : яване на страх) и в много случаи предоставят повече информация за автора на съответната програма.

Обща информация за вирусите част 2-ра

- Разбирането на основните положения при злонамерен софтуер ще помогне на много потребители да избягват инциденти с такива програми, както и да различават истинската заплаха от обикновените шеги, измамни закачки или нормални предупреждения на системата. Например съобщението за грешка от общ характер в защитата (General Protection Fault — GPF), установявана от програмата Dr. Watson, е нещо, което опитният потребител ще разпознае като нормална част от живота на работна среда под Windows. Неопитният потребител обаче винаги се опасява от най-лошото и може да интерпретира GPF като заразяване с вирус. Придобиването на грамотност за основите на компютъра, софтуерната конфигурация, конфликтите и програмните грешки (т. нар. „бъгове") е част от дългия път към получаване на удовлетворение от работата с компютри.
- Бъговете също не се причисляват към злонамерения софтуер. „Бъг" се нарича програмна грешка, която води до частичен или пълен отказ на изпълнение на програмата. Произходът на думата „бъг" (bug — букв. „бръмбар") обикновено се свързва с екип от личности, работили с професор Хауърд Ейкън в Харвард, които открили, че късото съединение в захранването на компютъра „Mark I" е причинено от молец. В повечето случаи програмистите използват софтуер за откриване на програмни грешки (т. нар. „дебъгери"), за да намират и поправят грешки в кода, преди да пуснат нова или актуализирана версия на дадена програма.
- Добре познатият „проблем 2000" (Y2K) не е нито бъг, нито злонамерен софтуер. На практика това е резултат от недобре обмислена „рационализация". Вместо да следят всичките четири цифри на годината, например 1979, програмистите създавали програми, отчитащи само последните две цифри — „79" за 1979 г. Когато работят в много кратки срокове, програмистите нямат никакво време да се безпокоят за такива „дреболии" и мислят само за наближаващия краен срок за завършване на проекта. За съжаление много производители продължават да използват този „рационализиран" код и в началото на 90-те години, което доведе до скъпоструващи надстройки на всичко, работещо на компютри или чипове, които не са съвместими с Y2K. За щастие посрещането на новата 2000 година не бе помрачено от Y2K; имаше съобщения за единични проблеми в световен мащаб. (Някои автори вече споменават за „Y10K" — проблем на 10 000-та година, но това е по-скоро в кръга на шегата. Бел. прев.)
- Компютърни вируси
- Компютърен вирус е програма, предназначена да се репродуцира, разпространява от компютър на компютър чрез програми-гостоприемници, и понякога да извършва зловредно действие. (Това е т. нар. „полезен товар" — payload. Тъй като действието на вирусите в никакъв случай не

Обща информация за вирусите част 2-ра

- може да се окачествти като „полезно", ще използваме понятието „ефективен товар" или само „товар" — бел. прев.) Налични са различни типове вируси с многообразни характеристики за избягване на разпознаване, възпроизвеждане и доставяне на ефективен товар на един компютър.
- Конвенция за имена
- Компютърните вируси имат най-различни имена, като някои носят в себе си повече смисъл от други. Въпреки че в началото на 90-те години групата CARO, съставена от множество елитни антивирусни изследователи, се опита да установи конвенция за имената на вирусите, понастоящем няма общоприет международен стандарт за именуване на новооткрития злонамерен софтуер. Например дадена антивирусна програма може да докладва за наличие на вирус V-Sign, а друга да означава същия вирус като Cansu. За щастие повечето компании възприемат подобни имена непосредствено след откриване на нов вирус. Например вирусът Concept се среща и като WM.Concept.
- Водещите компании в областта на антивирусната защита като Symantec публикуват своите конвенции за именуване в Интернет. Symantec дава имена на всички вируси, като поставя представка, обозначаваща платформата за репродуциране, името на семейство, и наставка — за варианти в семейството, ако има такива. Например WM.Concept.C означава макровирус за Word (Word Macro) от семейство Concept, вариант C.
- Как се репродуцират вирусите?
- Вирусите се притаяват в очакване на даден компютър, като при изпълнение (стартиране) се репродуцират на локално или мрежово устройство. В настоящия момент хиляди вируси стоят „в засада" върху компютри по цял свят, в очакване да бъдат изпълнен. След като кодът бъде стартиран, вирусът може да зарази системата и да се разпространи върху други файлове, дискове (включително устройства, достъпни през мрежа), сектори за начално зареждане и друга компютърна среда.
- Изпълнение на кода
- Всеки път когато в една система бъде внесен нов носител на информация, той я подлага на риск от заразяване с вируси. Когато потребителят изпълнява действие като отваряне на нов файл, използване на дискета или стартиране на изтеглена от Интернет програма, може да започне изпълняване на вирусен код, като позволява на вируса да се разпространи и да зарази цялата система.

Автор:**LORD OF DARK**
Ц. Угринов

Skype: LORDOFDARK E-Mail: info@virusinfo-bg.org

Седмично електронно списание за компютърна сигурност

- Благодарости на ASpace, че се съгласи да се включи в този брой на списанията и се надяваме и за напред да се включва и да дава полезна информация.
- Специална благодарност и на mihnev_sz за статията.
- Virus Info се спонсорира с любезното съдействие на Eset.bg
- Други проекти на Bulgarian Portal Network:
  - www.potal-bg.info Софтуерни новини
  - www.bg-windows.info Помощ за Windows, статии, новини, трикове и други

Bulgarian Security Research Portal:

info@virusinfo-bg.org Информация, запитвания и проблеми.

newvirus@virusinfo-bg.org нови вируси, заплахи и съмнителни файлове изпращайте тук.