Сигурност на Internet Explorer

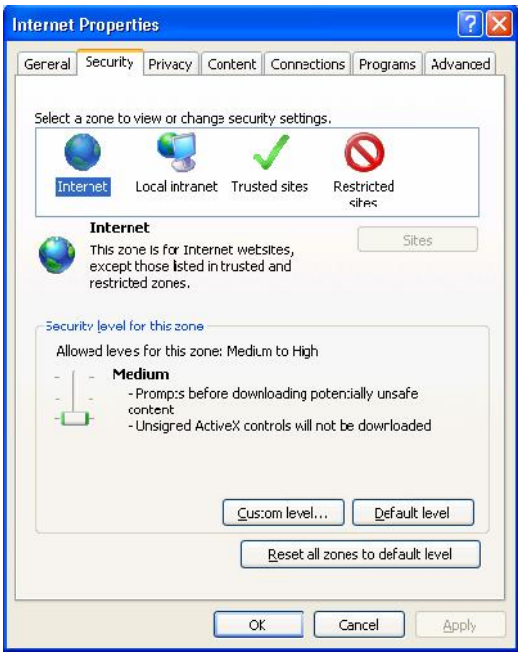
Една от най-важните характеристики на интернет браузърите е тяхната сигурност, За това тук разглеждаме този как стоят нещата по този въпрос при Internet Explorer. Темата е разделена на три основни точки:

- Сигурност
- Уязвимост на защитата
- Настройки

Сигурност

Internet Explorer съдържа пет предварително зададени зони за сигурност:

- "Интернет" (Internet),
- "Локален интранет" (Local Intranet),
- "Надеждни сайтове" (Trusted Sites),
- "Ограничени сайтове" (Restricted Sites)
- "Моят компютър" (My Computer).



Можете да конфигурирате зоната "Моят компютър" (My Computer) (която съдържа файловете, намиращи се на вашия компютър) само с пакета за администриране на Microsoft Internet Explorer (Microsoft Internet Explorer Administration Kit, IEAK), тъй като тези настройки липсват в интерфейса на браузъра. Администраторите трябва да използват настройките по подразбиране за тази зона, освен ако организацията няма специфично изискване. По-ниските настройки за сигурност създават риск за сигурността, докато по-високите нива могат да ограничат функционалността на браузъра.

Можете да зададете желаните опции за сигурност за всяка зона, след което да добавяте или премахвате сайтове от зоните, в зависимост от нивото на доверие, което имате към съответния уеб сайт.

Видове зони за сигурност

Интернет зона (Internet Zone)

Тази зона съдържа уеб сайтове, които не са записани нито на вашия компютър, нито в локалната интранет мрежа, както и тези, които не са вече определени към друга зона. Нивото за сигурност по подразбиране е "Средно" (Medium).

Зона на локалния интранет (Local Intranet Zone)

По подразбиране, зоната на локалния интранет съдържа всички мрежови връзки, създадени с помощта на път от тип "Универсална конвенция за именуване" (Universal Naming Convention, UNC), и уеб сайтовете, които заобикалят прокси сървърите или имат имена, които не включват точки (например http://local), при условие, че не са определени към зоните "Ограничени сайтове" (Restricted Sites) и "Надеждни сайтове" (Trusted Sites). Нивото по подразбиране за зоната "Локален интранет" (Local Intranet) е "Средно" (Medium) (Internet Explorer 4) или "Средно ниско" (Medium-low) (Internet Explorer 5 и 6). Забележете, че можете да осъществявате достъп до споделени ресурси в локална мрежа или интранет, както и до уеб сайт в интранет посредством адрес от вида "Интернет

протокол" (Internet Protocol, IP) или с помощта на пълно име на домейна (FQDN), при което споделения ресурс или уеб сайта се определя, като намиращ се в зоната "Интернет" вместо в зоната "Локален интранет".

Зона с надеждни сайтове (Trusted Sites Zone)

Тази зона съдържа уеб страници, които смятате за безопасни (например уеб сайтове в интранета на вашата организация или на известни компании, на които се доверявате). Добавянето на уеб сайт към зоната с надеждни сайтове се базира на предположение, че файловете, които изтегляте или стартирате от уеб сайта, няма да навредят на компютъра или данните. По подразбиране няма уеб сайтове, които да са поставени в зоната с надеждни сайтове, а зададеното ниво на сигурност е "Ниско" (Low).

Зона с ограничени сайтове (Restricted Sites Zone)

Тази зона съдържа уеб сайтове, които считате за ненадеждни. Добавянето на уеб сайт към зоната с ограничени сайтове се базира на предположение, че файловете, които изтегляте или стартирате от уеб сайта, могат да увредят компютъра или данните. По подразбиране няма уеб сайтове, които да са поставени в зоната с ограничени сайтове, а зададеното ниво на сигурност е "Високо" (High).

Зоната с ограничени сайтове (Restricted Sites) съдържа уеб сайтове, които не са записани нито на вашия компютър, нито в локалната интранет мрежа, нито вече са определени към друга зона. Нивото за сигурност по подразбиране е "Средно" (Medium).

Забележка Настройките за сигурност се прилагат само към файлове, които се намират в папката "Временни Интернет файлове" (Temporary Internet Files) на компютъра. Тези настройки използват нивото за сигурност на сайта, от който са получени файловете. Всички други файлове ще бъдат считани за безопасни.

Уязвимост на защитата

През годините Internet Explorer е бил подложен на много проблеми в защитата и голяма част от тях се отнасят за: шпионски софтуер, рекламен софтуер и компютърни вируси. Всички тези изброени през Интернет са възможни от заради бъгове и грешки в архитектурата на сигурността на Internet Explorer, което понякога налага нищо повече от гледане на злонамерена уеб страница, за да се заразите. Това е известно като ""drive-by install"". Те също така се опитват да измамят потребителя с инсталиране на зловреден софтуер, като погрешно, е описана истинската цел на софтуера в съобщението тревога на сигурността на ActiveX.

Няколко пропуска в сигурността, засягащи IE не са възникнали в самият браузър, но в ActiveX-базирани добавки, използвани от него. Тъй като добавки имат същите привилегии като IE, недостатъците може да са толкова критични, каткто тези на самият браузър. Това е довело до много критики за ActiveX-базираната архитектура и се е смятало че е била доста податлива на атаки. До 2005 г., някои експерти твърдят, че опасностите от ActiveX са били надценени и е имало взети предпазни мерки преди това. През 2006 г., нови техники за използване автоматизирано тестване са открили повече от сто уязвимости в стандартните компоненти на Microsoft ActiveX за сигурността. Въведенията след това в наскоро публикувания в Internet Explorer 7 смекчават някои от тези уязвимости.

Internet Explorer през 2008 г. вече има известен брой публикувани уязвимости в сигурността. Според изследване направено от изследователската компания за сигурност Secunia, Microsoft не реагира толкова бързо, колкото конкурентите си при определяне на дупки в сигурността и като кръпки. Фирмата също докладвани 366 уязвимости в контрола, което е увеличение от предходната година.

Според последната информация, Secunia съобщава, че IE6 има 24 известни незакърпени уязвимости, IE7 има 11, и IE8 е 4. Най-тежко незакърпени дупки Secunia, засягащи Microsoft Internet

Explorer 6.x, 7.x, 8.x и с всички оператори лепенки приложени, са оценени изключително критично. Най-старият известен незакърпени уязвимости за IE6, IE7 и IE8 датата, от 7-ми Ноември 2003 г., 6 юни 2006 г., и 26-ти февруари 2007 съответно.

Според последната информация, сигурност изследователската компания SecurityFocus съобщава, че IE6 е 396 известни незакърпени уязвимости, IE7 е 22, както и IE8 е 25. Най-старият известен незакърпени уязвимости за IE6, IE7 и IE8 дата от 20 ноември 2000 година, 17-ти май 2007 г, и 11-ти април, 2009 год. съответно.

Internet Explorer е критикувана от един Evan за Крис е известно уязвимост на сигурността, които може да допусне разкриване на информация да останат незаписани за най-малко 600 дни. [68] Microsoft казва, че е знае за тази уязвимост, но тя е с много ниска тежест като сайт жертвата в Мрежата трябва да бъде конфигуриран по специален начин за тази атака да бъде възможно на всички.

През декември 2010 г., учените са успели да заобиколят функцията "защитеният режим" в Internet Explorer.

Настройки

Конфигуриране на зоните за сигурност

За да промените нивото на сигурност по подразбиране, персонализирайте опциите за сигурност в зона или присвоете уеб сайт на конкретна зона. За целта изпълнете стъпките, описани в един от разделите по-долу.

Промяна на нивото на сигурност по подразбиране за зона

За всяка зона за сигурност в Internet Explorer 4.x можете да изберете ниво на сигурност "Високо" (High), "Средно" (Medium), "Ниско" (Low) или "По избор" (Custom). В Internet Explorer 5 и 6 можете да изберете следните настройки на нивата за сигурност: "Високо" (High), "Средно" (Medium), "Средно ниско" (Medium-low), "Ниско" (Low) или "По избор" (Custom).

За да промените нивото на сигурност по подразбиране за зона:

1. В Internet Explorer 4.x натиснете **"Опции за Интернет" (Internet Options)** в менюто**"Изглед" (View)**. В Internet Explorer 5 и 6 натиснете **"Опции за Интернет" (Internet Options)** в менюто **"Инструменти" (Tools)**.
2. В раздела **"Защита" (Security)** на Internet Explorer 4.x щракнете върху зоната, на която искате да промените нивата за сигурност, в полето **"Зона" (Zone)**.

   В раздела **"Защита" (Security)** на Internet Explorer 5 и 6 под фразата **"Изберете зона на Web съдържание, за да укажете нейните настройки за защита" (Select a Web content zone to specify its security settings)** щракнете върху зоната, на която искате да присвоите уеб сайт.
3. Щракнете върху нивото на сигурност, което искате да се използва за зоната, след което натиснете **OK**.

Персонализиране на настройките за сигурност на зона

Опцията "По избор" (Custom) предоставя на опитните потребители и администратори повече контрол върху всички опции на защитата. Например опцията "Изтегляй неподписани ActiveX контроли" (Download Unsigned ActiveX Controls) е деактивирана по подразбиране в зоната на локалния интранет (в тази зона средното ниво (Medium) е нивото на сигурност по подразбиране). В този случай Internet Explorer може да не задейства никакви ActiveX контроли в интранета на вашата организация, защото повечето организации не подписват ActiveX контроли, които се използват само вътрешно. За да може Internet Explorer да стартира неподписани ActiveX контроли в интранета на вашата организация, за зоната на локалния интранет сменете нивото на сигурност в опцията **"Изтегляй неподписани ActiveX контроли" (Download Unsigned ActiveX**

Controls) с **"Подкана" (Prompt)** или**"Разреши" (Enable)**. Можете да зададете следните опции на сигурност с помощта на настройката **"По избор" (Custom)**:

- Достъп до файлове, ActiveX контроли и скриптове
- Нивото на функционалност, предоставено за Java програми
- Дали сайтовете трябва да бъдат идентифицирани чрез протокола за автентификация (удостоверяване) Secure Sockets Layer (SSL)
- Защита с парола чрез използване на протокола Windows NT Challenge/Response (NTLM) В зависимост от това, в коя зона се намира сървъра, Internet Explorer може автоматично да ви предоставя паролата, да поисква въвеждането на вашето потребителско име и парола, или да отказва всички опити за влизане

За да персонализирате опциите за сигурност на зона:

1. В Internet Explorer 4.x натиснете **"Опции за Интернет" (Internet Options)** в менюто**"Изглед" (View)**.

   В Internet Explorer 5 и 6 натиснете **"Опции за Интернет" (Internet Options)** в менюто **"Инструменти" (Tools)**.
2. В полето **"Зона" (Zone)** на раздела **"Защита" (Security)** на Internet Explorer 4.x щракнете върху зоната, която искате да персонализирате.

   В раздела **"Защита" (Security)** на Internet Explorer 5 и 6 под фразата **"Изберете зона на Web съдържание, за да укажете нейните настройки за защита" (Select a Web content zone to specify its security settings)** щракнете върху зоната, на която искате да присвоите уеб сайт.
3. Щракнете върху **"Настройки на потребителя, за опитни потребители" (Custom (For Expert Users))**, след което натиснете **"Настройки" (Settings)**.

   В Internet Explorer 5 и 6 щракнете върху **"Ниво по избор" (Custom Level)**.
4. Под **"Възстановяване на персонализираните настройки" (Reset Custom Settings)** щракнете върху нивото на сигурност за цялата зона в полето **"Възстанови ниво" (Reset To)**, след което натиснете **"Възстанови" (Reset)**.
5. Под раздела, за който искате да персонализирате настройките за сигурност, щракнете върху желаната опция, натиснете **OK** и пак **OK**.

За присвояване на уеб сайт към конкретна зона за сигурност:

1. В Internet Explorer 4.x натиснете **"Опции за Интернет" (Internet Options)** в менюто**"Изглед" (View)**.

   В Internet Explorer 5 и 6 натиснете **"Опции за Интернет" (Internet Options)** в менюто **"Инструменти" (Tools)**.
2. В полето **"Зона" (Zone)** на раздела **"Защита" (Security)** в Internet Explorer 4.x щракнете върху зоната, на която искате да присвоите уеб сайт, след което натиснете**"Добави сайтовете" (Add Sites)**.

   В раздела **"Защита" (Security)** на Internet Explorer 5 и 6 под фразата **"Изберете зона на Web съдържание, за да укажете нейните настройки за защита" (Select a Web content zone to specify its security settings)** щракнете върху зоната, на която искате да присвоите уеб сайт, след което натиснете бутона**"Сайтове" (Sites)**.

   Ако добавяте сайт към зоната на локалния интранет, можете първо да изберете какви видове уеб сайтове, искате да се добавят към зоната, след което натиснете бутона**"Разширени" (Advanced)**, за да добавите конкретни сайтове. Следните правила важат за опциите на

зоната на локалния интранет. Имайте предвид, че добавянето на сайт към която и да е зона получава по-висок приоритет от следните правила:

- "Включи всички локални (интранет) сайтове, които не са в списъците на другите зони:" (Include all local (intranet) sites that are not listed in other zones:) Имената на интранет сайтовете не включват точки (например http://local). Име на сайт, като например http://www.microsoft.com, не е локално, защото съдържа точки. Този сайт се присвоява на зоната "Интернет" (Internet). Правилото за името на интранет сайтовете се отнася както за "file:", така и за "http:" адреси. Имайте предвид, че достъпът до Интернет домейни от най-високо ниво може да става с помощта на имена, които не съдържат точки. Ако имате достъп към обикновените домейни (.com, .org, .net, .edu, .gov, .mil или .int) или към домейни, съдържащи кодове на държави (.us, .jp, .uk и т.н.), отстранете отметката от тази опция, за да не позволявате на тези сайтове да използват настройките за сигурност на зоната "Локален интранет" (Local Intranet). За допълнителна информация относно домейните от най-високо ниво, посетете следния сайт на Internet Corporation For Assigned Names and Numbers (ICANN):

  http://www.icann.org/tlds

- "Включи всички сайтове, които заобикалят прокси сървъра:" (Include all sites that bypass the proxy server:) Типичните интранет конфигурации използват прокси сървър за достъп към Интернет и директна връзка към интранет сървърите. Настройката използва този тип конфигурационна информация, за да различава интранет и Интернет съдържание с цел зониране. Ако прокси сървърът е конфигуриран по различен начин, махнете отметката от тази опция и използвайте други опции, за да определите, кои файловете ще се присвояват на зоната "Локален интранет" (Local Intranet). На компютрите без прокси сървър тази настройка няма влияние.
- "Включи всички пътища на мрежата (UNCs):" (Include all network paths (UNCs):) Мрежовите пътища (например \\local\file.txt) обикновено се използват за съдържание на локалната мрежа, което трябва да е включено в зоната на локалния интранет. Ако има мрежови пътища, които не бива да се намират в зоната на локалния интранет, махнете отметката от тази опция и използвайте други опции, за да определите, кои файловете ще се присвояват на тази зона. Например в определени конфигурации от тип Common Internet File System (CIFS) е възможно мрежов път да представлява препратка към Интернет съдържание.

3. Въведете уеб адрес в полето **"Добави този уеб сайт в зоната" (Add this Web site to the zone)** и натиснете бутона **"Добави" (Add)**.
4. Натиснете **OK** и после отново **OK**.

При добавянето на сайтове в зоните "Локален интранет" (Local Intranet) или "Надеждни сайтове" (Trusted Sites) можете да изискате да се използва сървърна проверка, като изберете опцията **"Изисквай проверка на сървъра (https:)" (Require server verification (https:)) за всички сайтове в тази зона" (for all sites in this zone)**.

Забележка Не можете да присвоите уеб сайт на зоната "Интернет" (Internet). Зоната "Интернет" съдържа всички уеб сайтове, които не са записани нито на вашия компютър, нито в зоната на локалния интранет, нито които вече са присвоени на друга зона.

За допълнителна информация относно разрешаването на проблеми, които не бяха елиминирани при предишните стъпки, щракнете върху следния номер на статия в базата знания на Microsoft:
319585 Съобщение за грешка "Software update incomplete" ("Незавършена актуализация на софтуера") при посещение на сайта Windows Update