



حقوق دسترسی را با چشم باز تعیین کنید

یک شبکه خوب، یک شبکه ایمن است

فضایی از یک رایانه که معمولا سرور است به عنوان فضای شیرینگ در نظر گرفته می شود و همه رایانه ها از این فضا استفاده می کنند و رایانه ها فضای به اشتراک گذاشته شده ای نخواهند داشت.

در سیستم های بزرگ تر معمولا از نرم افزارهای اختصاصی برای مدیریت فایل شیرینگ استفاده می کنند.

مدیریت اتصالات

پس از راه اندازی شبکه با رعایت اصول ایمنی، فردی باید مسئولیت نظارت دائم و یا دوره ای رایانه های متصل با شبکه را برعهده بگیرد چراکه بدافزارها و نفوذگران از روش های مرسوم اتصال با رایانه استفاده نمی کنند و ممکن است به طریقی به رایانه راه یابند که یا کاملا مخفی است و یا به ظاهر بی خطر و کنترل شده است؛ از همین رو استفاده از ابزارهای امنیتی مانند فایروال و آنتی ویروس در رایانه های یک شبکه ضروری است. البته اتکای مطلق به فایروال و آنتی ویروس کاری نیست که حرفه ای ها انجام می دهند اما استفاده از این ابزار می تواند کار نظارت را آسان تر کند.

توجه به این موضوع ضروری است که همه برنامه های موجود در رایانه های یک شبکه نیازی به اتصال به شبکه ندارند. استفاده از فایروال ها در سرور می تواند نظارت بر ارتباطات برنامه ها در کلاینت ها را آسان تر کند. کسری پاکینیت

هیچ پوشه یا فایل را Share نکنید، در غیر این صورت با فعال کردن سربرگ Security، پوشه های مورد نیاز را برای اعضا Share کنید و نه برای کل Workgroupe. چرا که در صورتی که هکر بتواند به تنظیمات شما پی ببرد می تواند مانند یکی از اعضای Workgroupe به اطلاعات دسترسی یابد.

در مراحل بالاتر امنیتی می توانید برای دادن دسترسی به کاربران با استفاده از ویندوز سرور، کلمات عبور تعیین کنید اما این کار پیچیدگی را تا حد زیادی افزایش می دهد و بیشتر برای شبکه های بسیار بزرگ مناسب است.

محدودیت در تعداد کاربران

طبیعی است که وقتی حدود دسترسی را برای کاربران ویندوز و نه برای IPها تعیین می کنید، تعداد کاربران شبکه محدودتر خواهد شد. هر اندازه که تعداد کاربران یک شبکه افزایش یابد، امنیت آن نیز بیشتر تهدید می شود اما این تهدید زمانی تشدید خواهد شد که تعداد کاربرانی با حق دسترسی Admin نیز افزایش یابد.

برای رایانه های متصل به شبکه، نام های کاربری با سطح دسترسی پایین Limited ایجاد کنید و سپس حقوق دسترسی در شبکه را برای این کاربری ها تعریف کنید.

استفاده از محیط شیرینگ واحد

وقتی تعداد رایانه های یک شبکه افزایش یابد به تبع میزان تبادل اطلاعاتی و شیرینگ ها نیز افزایش خواهد یافت. در این صورت هر پوشه به اشتراک گذاشته شده مستعد میزبانی یک بدافزار خواهد بود. برای کاهش خطر و قابل کنترل کردن این اتفاق،

درست از زمانی که شبکه های رایانه ای پا به خلقت گذاشتند، امنیت در شبکه اهمیت یافت. ایجاد نرم افزارهای کنترل شبکه موسوم به فایروال این اهمیت را نشان می دهد. فراگیری روش هایی برای ایمن سازی شبکه های رایانه ای برای متخصصان موضوعی جدی است و باید حداقل اصول ایمن سازی شبکه را بیاموزند.

در این فصل نیز شبکه های خانگی بیشتر از گذشته رواج می یابند. بد نیست که برخی از اصول ایمن سازی شبکه را مرور کنیم.

تنظیمات دقیق دستی

کافی است دو یا چند رایانه را از طریق کابل شبکه به هم وصل کنید تا همه چیز به خودی خود به کار افتد اما امنیت چیزی نیست که خود به خود فراهم شود. حرفه ای ها برای هر رایانه IP ثابت در نظر می گیرند تا در آینده بتوانند با چشمانی باز شبکه را مدیریت کنند. معمولا رایانه های شبکه های محلی، IPهایی در حدود 10.1.x.x و 192.168.x.x را به خود اختصاص می دهند. در صورتی که شبکه به اینترنت متصل است، اختصاص IPهایی در بازه های دیگر می تواند شناسایی شبکه داخلی را برای مهاجمان احتمالی خارجی سخت تر و شبکه را ایمن تر سازد. در ویندوز سرور و یا نسخه های حرفه ای ویندوز، اختصاص دامین به شبکه، امنیت را تا چندین برابر تقویت می کند اگر چه این کار مخصوص حرفه ای های شبکه است.

اعمال محدودیت

شبکه ها با اهداف خاصی راه اندازی می شوند پس هر کاربر باید تنها به اندازه دسترسی داشته باشد که برای رسیدن به هدف شبکه نیازمند است. اگر قرار نیست هیچ فایل یا در میان شبکه رد و بدل شود،

ترفند ویندوز

رادار رازدار مشکلات رایانه



در ادامه مبحث ارائه ترفندهای ویندوز هفت قصد داریم ترفندی کاربردی برای اشکال یابی فنی رایانه را برای شما شرح دهیم. در این ترفند شما را با یکی از قسمت های کنترل پنل آشنا می سازیم که تاکنون کمتر نام آن را شنیده اید.

این قسمت که View reliability history نام دارد زیرمجموعه ای از قسمت Action Center می باشد. همچنین این مرکز کنترل از منوی استارت هم قابل دسترسی است.

به طور کلی این قسمت، تمامی مشکلات اتفاق افتاده در رایانه شما را با جزئیات درون خود ثبت می کند و در هر لحظه قادر خواهید بود به جزئیات مشکلات گذشته رایانه خود دسترسی پیدا کنید.

کاربر با کلیک روی هر یک از مشکلات ثبت شده و یا علائم خطر می تواند جزئیات آن پدیده ثبت شده را مشاهده کند.

توجه داشته باشید که مشکلات ثبت شده در رایانه شما در این قسمت به طور دسته بندی شده مشاهده می شوند که دسته بندی ها در کنار جدول قابل مشاهده اند. به عنوان مثال در صورتی که در مقابل Application Failures علامتی ثبت شده باشد، در صورت کلیک کردن روی علامت مذکور فهرست برنامه هایی که در آن روز به صورت ناگهانی بسته شده اند را مشاهده خواهید کرد و با زدن روی عبارت Check for a solution می توانید راه حل های موجود و معتبر را دریافت کنید.

این پنجره ویژگی هایی دیگر را نیز در خود جای داده است. به عنوان مثال می توانید این اطلاعات را به صورت فایلی با پسوند XML ذخیره و آن ها را ارسال، ویرایش و یا آنالیز کنید.

برای انجام این کار روی گزینه reliability history Save کلیک کرده و فایل مذکور را در آدرس دلخواه خویش ذخیره کنید.

در صورتی که مایل به جستجوی راه حل برای تمامی مشکلات باشید می توانید روی گزینه Check for solutions to all problems کلیک کنید.

توجه داشته باشید که اشکال یابی در ویندوز هفت از راه های دیگری نیز انجام می شود که این راه، از کامل ترین آن هاست.

ترفند جاوا اسکریپت

رویداد onload در JQuery (قسمت دوم)

در شماره قبل به طور مختصر با یکی از روش های پیاده سازی رویداد ready آشنا شدیم. همان طور که گفته شد این رویداد پس از این که تمام بخش های ضروری صفحه یا به طور دقیق تر DOM بارگذاری شد فراخوانده می شود. در این شماره قصد داریم مثال هایی را با کمک این رویداد پیاده سازی کنیم:

```
<html>
<head>
<script src="js/jquery-1.4.2.min.js"></script>
<script>
$(document).ready(function () {
$("p").text("The DOM is now loaded and can be manipulated.");
});
</script></head><body>
<p>Not loaded yet.</p>
</body>
</html>
```

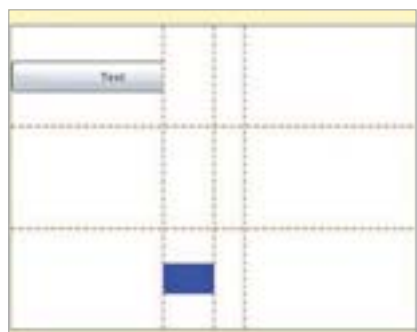
مثال فوق که مثال کلاسیک JQuery برای رویداد



ترفند وب

کار با Max-Width در مرورگرهای مختلف (قسمت سوم)

به عنوان مثال در صورتی که عبارت زیر استفاده شود: width:expression(150 + "px"); آن گاه این عبارت دقیقا برابر عبارت زیر می باشد: width:expression(150px); زمانی که کدهای HTML در صفحه IE اجرا می شوند دستور "px" + 150 خود به خود تبدیل به 150px خواهد شد بنابراین کفایت عبارت مناسبی برای قرار گرفتن در بخش expression پیاده سازی کنیم. لازم به ذکر است این خاصیت تنها در مرورگر IE قابل استفاده می باشد.



همان طور که در شماره قبل مشاهده کردید خصوصیاتی مانند max-width و max-height در یک مرورگر غیراستاندارد مانند IE کار نمی کنند؛ در نتیجه برای داشتن چنین خصوصیاتی باید به دنبال یافتن راه حل دیگری باشیم.

یکی از راه حل های پیشنهادی، استفاده از کدهای جاوا اسکریپت است؛ کدی که با کمک آن سایز یک کنترل را (چه در width و چه در height) همواره در حد مشخصی نگه داریم اما از آن جا که استفاده از جاوا اسکریپت نیازمند داشتن مهارت های خاص آن است ترجیح می دهیم که از راه حل استفاده کنیم که در آن کمتر از جاوا اسکریپت استفاده شده باشد.

استفاده از Expression در CSS

سازنده های مرورگر IE سعی کرده اند ضعف های مرورگر خود را با راه حل های مختلفی بپوشانند. بدین طریق روش های جدیدی در طراحی وب به وجود آمده که تنها مختص IE است. یکی از این روش ها استفاده از Expression است. با کمک Expression طراح وب می تواند لایه لایه کدهای CSS تک ای کد جاوا اسکریپت بنویسد. درباره Expression در فرصتی دیگر بحث خواهیم کرد اما به طور خلاصه در این مسئله خاص می توانیم اندازه خصوصیت Width کنترل مورد نظرمان را با کمک یک تکه کد ساده جاوا اسکریپت (که در حقیقت یک عبارت محاسباتی محسوب می شود) که درون عبارت Expression استفاده شده است به طور پویا تغییر دهیم.

شکل کلی این نوع استفاده به شکل زیر خواهد بود:

width:expression(some javascript codes);