**آشنایی با مفاهیم امنیت در مجازی سازی**

**10 دلیل برای بالا بردن امنیت توسط مجازی سازی**

مجازی سازی نوعی فرآیند برای ایجاد یک محیط مجازی است که در حقیقت به کاربر اجازه اجرای سیستم عامل های چند گانه بصورت همزمان بر روی یک کامپیوتر را می دهد. ایجاد این نسخه مجازی بجای حقیقی می تواند در غالب ویندوز سرور و یا منابع شبکه باشد. برای بسیاری از شرکت ها و سازمان ها مجازی سازی می تواند به عنوان بخشی از یک روند اصلی در محیط های فناوری اطلاعات باشد که توانایی محاسبات نرم افزاری براساس فعالیت های درک شده را داراست. مهمترین و اصلی ترین هدف مجازی سازی کاهش وظایف اداری است این در صورتی است که نباید منکر تاثیرات بالقوه بر بهبود مقیاس پذیری سازمانی و کاهش حجم کار شد با این محسنات می توان از مجازی سازی برای بهبود امنبت استفاده نمود در این مقاله ما به 10 نکته برای به حداقل رساندن حملات و بهبود امنیت برای بهره مندی کامل از مجازی سازی اشاره می نمائیم.

**مجازی سازی و امنیت**

بسیاری از سازمانها پس از اعمال تکنولوژی های جدید در مورد پیامدهای امنیتی و چگونگی و احتمال حملات به شبکه خود تحقیق می کنند. از پیامدهایی که مجازی سازی می تواند برای شما به ارمغان بیاورد می توان به: صرفه جویی در هزینه ها، افزایش بهره وری در کار، کار بیشتر با تجهیزات کمتر و پائین آوردن زمان خرابی و توقف فعالیت در شبکه را نام برد. از انواع مجازی سازی می توان به مجازی سازی شبکه Network Virtualization مجازی سازی ذخیره سازی Storage Virtualization مجازی سازی برنامه Application Virtualization مجازی سازی دسکتاپ Desktop Virtualization مجازی سازی سرور Server Virtualization را نام برد. البته لازم به ذکر است پیاده سازی هر نوع از مجازی سازی ها می تواند نوعی خطر امنیتی در بر داشته باشد اما مهم این است که مجازی سازی می تواند امنیت را بهبود ببخشد اما توانایی جلوگیری از حملات را ندارد. مجازی سازی می تواند در بسیاری از جهات مورد استفاده قرار گیرد اما نیاز به کنترل های امنیتی در سطح بالا را در هر شرایطی دارد در این مقاله ما سعی در معرفی راه های مختلف برای استفاده از مجازی سازی برای افزایش امنیت در محیط ویندوز را داریم.

**Sandboxing**

یک مکانیسم امنیتی پیشرفته برای جداسازی برنامه های در حال اجراست که اغلب برای اجرای کد یا برنامه های غیر از تست از طرف شخص ثالث، تامین کننده و وب سایت غیرمجاز استفاده می شود. هدف اصلی Sandboxing بهبود امنیت در مجازی سازی با جداسازی نرم افزار برای محافظت در مقابل بدافزارهای خارجی Malware، ویروس های مضر Harmful Viruses و ... است. گاهی اوقات ممکن است یک حمله مخرب به برنامه خود را در هنگام اجرای آن در یک مرورگر دریافت کنید بنابراین Sandboxing از سیستم عامل و برنامه ها در مقابل ویروس ها و یا حملات مضر به دستگاه مجازی محافظت می کند.

**Server Virtualization**

مجازی سازی سرور در اصل پنهان سازی منابع سرور است که در تقسیم بندی به سرورهای مجازی کوچکتر برای به حداکثر رساندن منابع کمک می نماید. ادمین شبکه سرور فیزیکی را به چندین محیط مجازی تقسیم می کند این امر به شما این اجازه را می دهد که سرورهای مجازی کوچک تر برای اجرای سیستم عامل و راه اندازی مجدد بصورت کاملا مستقل عمل نمایند و به هیچ عنوان در زمان اجرا نیازی به سیستم عامل دیگری نداشته باشند. این نوع از مجازی سازی عمدتا در سرورهای وب که خدمات میزبانی وب کم هزینه را ارائه می دهند مورد استفاده قرار می گیرد. با سرشکن نمودن منابع سرور می توانید با سرعت و دقت بیشتری عوامل مخرب مانند ویروس ها، باج افزارها و بدافزارها و ... را با سرعت بالاتری شناسایی و محافظت از سرورها و شبکه با سادگی بیشتری انجام خواهد شد. بزرگترین مزیت استفاده از مجازی سازی سرور این نکته است که یک لایه انتزاعی سخت افزاری بین سخت افزار X86 و سیستم عامل ایجاد می کند، همچنین چگالی سرورهای مجازی را به سخت افزار فیزیکی کاهش می دهد. به زبان ساده مجازی سازی سرور تعیین می کند که آیا سرور بصورت غیرمجاز عمل می کند یا خیر.

**Network Virtualization**

مجازی سازی شبکه ترکیبی از منابع شبکه سخت افزاری و نرم افزاری است و عملکرد شبکه را با یک شبکه مجازی مجزا ترکیب می کند، این امر تاثیرات بدافزارها را در هنگام آلوده شدن به حداقل می رساند. مجازی سازی شبکه با ایجاد لایه های مختلف در سخت افزار بصورت مجازی تناسبی منطقی را بین سخت افزار و نرم افزار بوجود خواهد آورد. یکی از ویژگی های مهم مجازی سازی Isolation است با استفاده از این فناوری یک ترکیب پویا از چندین شبکه مجازی بوجود خواهد آمد که برای راه اندازی سرویس های End-To-End بسیار موثر خواهد بود. یکی دیگر از ویژگی های اصلی مجازی سازی شبکه Segmentation یا تقسیم بندی است، این امر فرآیندی است که منجر به افزایش عملکرد یا به حداقل رساندن ترافیک محلی در شبکه و بهبود ساختار امنیتی شبکه داخلی از خارج خواهد شد. بنابراین مجازی سازی شبکه برای ایجاد یک زیر ساخت مجازی برای حمایت از نیازهای پیچیده با ایجاد نمونه های منحصر بفرد از برنامه های کاربردی نرم افزار برای سرویس دهی به مشتریان متعدد استفاده می شود.

**Hypervisor Security**

اصطلاح Hypervisor به معنای نرم افزار یا سخت افزار کوچک است که ماشین های مجازی را ایجاد و اجرا می کند. دستگاهی که حاوی Hypervisor است دستگاه میزبان یا Host Machine نامیده می شود. برخی از توصیه های کلیدی امنیتی برای Hypervisor:  
آپدیت های Hypervisor منتشر شده توسط ارائه کننده را نصب نمائید البته اکثر این Hypervisor ها بروزرسانی خودکار نرم افزار را داشته و بروزرسانی ها را پیدا خواهد کرد.  
امنیت با Hypervisor باعث می شود استقرار آسان و کارآمد و در اجرا به حداقل هزینه ها کاهش یابد.  
اگر شما نیازی به سرویس به اشتراک گذاری فایل یا هر سرویس دیگر بین سیستم مهمان و سیستم عامل میزبان ندارید، هر سرویسی را که مورد نیاز نیست را غیرفعال نمائید برای برقراری کمترین نقاط اتصال.  
باید بین سیستم عامل و مهمان امنیت برقرار باشد تا این ارتباط بصورت Stable بوجود آید. محیط های غیرمجازی باید توسط کنترل های امنیتی نظیر فایروال، آنتی ویروس های تحت شبکه و غیره انجام شود.

**Desktop Virtualization**

مجازی سازی دسکتاپ برای ایجاد، اصلاح یا حذف تصاویر به شما آزادی عمل می دهد و محیط دسکتاپ را از رایانه فیزیکی که برای دسترسی از آن استفاده می شود جدا می سازد و دسکتاپ کاربر را دقیقا به دسکتاپ محلی او تبدیل می نماید.

**Infrastructure Security**

زیرساخت اطلاعات مجازی کنترل دسترسی به منابع و حفظ و امنیت اطلاعات را بعهده دارد.

**Virtual Switches**

سوئیچ مجازی، یک نرم افزار برای استفاده از تکنیک های Isolation، کنترل و بازرسی محتویات بین ماشین های مجازی، امنیت را فراهم می سازد و اجازه ارتباط با دیگر ماشین ها را برقرار می سازد.

**Guest OS Security**

این سیستم عامل در یک ماشین مجازی است و برای میزبانی سیستم عامل اصلی و به اشتراک گذاشتن منابع با سایر ماشینهای مجازی در همان میزبان استفاده می شود. مجازی سازی این اجازه را به شما می دهد که اشتراک گذاری اطلاعات با سیستم عامل توسط دیسک یا پوشه ایجاد شده یا دیسک های شبکه انجام پذیرد که این امر شامل برخی از ویژگی های امنیتی مانند به روز رسانی OS مهمان سیستماتیک، سیستم بک آپ از درایوهای مجازی و استفاده از همین سیاست برای کامپیوترهای مجازی سازی نشده.

**High Availability And Disaster Recovery**

امروزه مهمترین مسئله در فناوری اطلاعات حفظ نمودن اطلاعات در بخش IT است. مجازی سازی زمان و هزینه بازیابی در زمان خطر را با استفاده از نسخه پشتیبان گیری و بازگردانی و راه اندازی مجدد را کاهش داده و این اجازه را به شما می دهد که بتوانید با استفاده از نسخه پشتیبان آن ماشین را بر روی سرور دیگری راه اندازی نمائید.

**Server Isolation**

مجازی سازی از جداسازی سرور در درجه اول برای اهداف تجاری استفاده می کند سرورهای چندگانه را می توان در یک ماشین مجازی بدون مجازی سازی اجرا نمود اما در هنگام داشتن سرورهای چندگانه در یک سرور، خطر وجود خواهد داشت. مجازی سازی به شما این اجازه را می دهد که چندین سرور در یک سرور فیزیکی اجرا کرده در حالی که سرورها از یکدیگر جدا هستند زیرا در ماشین های مجزا در حال کار هستند.