باسمه تعالی

عنوان مستند

امنیت مجازی سازی

فهرست مطالب

۱ مقدمه

اجرای چندین ماشین مجازی روی یک کامپیوتر بجای سرورهای اختصاصی که هر کدام نیازمند نگهداری های دمایی و مراقبت های توان مصرفی است، مبحث متقاعدکننده ای است. گره های مجازی سازی شده که توسط یک سرور فیزیکی واحد تغذیه می شوند، صرفه اقتصادی مناسبی دارد. تأثیرات اقتصادی مجازی سازی می تواند به طرز جذابی قوی باشد. به استناد نظر سنجی انجام شده توسط Forrester در سال ۲۰۱۱، پیاده سازی زیرساخت های ماشین های مجازی ۲۵۵٪ از ریسک تنظیم شده در مدل ROI [۱] در یک بازه ی ۴ ساله را به همراه داشته است که حتی با یک بازدهی ۱۷ ماهه بعد از گسترش نیز برابر است.

اکنون سؤال این است که چه تعداد از ماشین های مجازی را می توان با آن مشخصات سخت افزاری بدون تأثیر قابل توجه در کارایی آنها پیاده سازی کرد؟ این به عنوان نرخ تثبیت شناخته می شود و این در حقیقت بخش ماهرانه کار است. با بسیاری از فاکتورهای که باید در نظر گرفته شود. به عنوان مثال باید دید ماشین مجازی مورد نظر چه نوع کارهایی را باید بتواند انجام دهد؟ از چه نرم افزاری برای ساخت استفاده می شود؟ ریسک های موجود برای سرمایه گذاری تمام عیار روی این کار چیست؟ و چگونه مطمئنانه زیرساخت مجازی خود را باید امن نمود و بدون کاهش بسیار زیاد سرعت در کار، از عدم آسیب پذیری در مقابل مجرمان مجازی اطمینان حاصل کرد؟ برای انتخاب تصمیم درست، به فهمیدن چندین مقوله و چگونگی ارتباط کاری بین آنها نیاز است.

۲ مدل های مجازی سازی

صنعت، مدل های مجازی سازی متنوعی تعریف کرده است. این گزارش سه مورد از این مدل ها را در نظر می گیرد:

مجازی سازی سرور ـ اجازه اجرای چند سیستم عامل را روی یک سرور به طور همزمان می دهد. این بهترین روش برای بهبود کارایی منابع سرور است. با بیش از ۸۰٪ کارایی در مقایسه با ماشین های سرور فیزیکی تک نقشی، که ۱۰ تا ۲۰ ٪ کارایی دارند.

مجازی سازی سرور سخت افزاری، تنها تهیه ی رابط میانی بین ماشین مجازی و سطح سخت افزار. ارزش بیشتری نسبت به مجازی سازی سرور بطور نرم افزاری دارد ـ جایی که سیستم عامل اصلی شامل قسمت های

[۱] Return on Investment

بیشتر مصرف کننده منابع هستند. به همین دلیل در بسیاری از کاربردهایی صنعتی ترجیح به استفاده از مجازی سازی سخت افزاری سرور است.

مجازی سازی دسکتاپ ـ سناریوهایی با ارزش های متفاوت را که با جابه جا کردن یک دسته از دسکتاپ های فیزیکی با زیرساخت کامپیوتر مجازی (VDI[۲]) است، ارائه می دهد. کلاینت های مقرون به صرفه، دسکتاپ های مبتنی بر نقش، شاخه های ریموت بی نیاز به سرویس های IT اختصاصی و نگهداری از صدها مکان کاری محدود به سرورهای فیزیکی که به خوبی مدیریت می شوند، شده اند.

مجازی سازی کاربرد ـ در این مورد بر خلاف زیرساخت یک دسکتاپ از راه دور مبتنی بر نقش، یک محیط مجازی فقط برای یک کاربرد خاص ساخته می شود. برای نرم افزار های در حال رشد سرویس دهنده، این یک انتخاب کارا و طبیعی است.

تمام مدل های مجازی سازی کاربردهای زیادی دارند و هر استفاده ای ریسک های مرتبط با خود را به همراه دارد. در این میان، ریسک های مربوط به تهدیدهای مجازی یکی از قابل توجه ترین هاست که در پیش گرفتن چند نمونه از راه حل های امنیتی را کاملاً ضروری می کند. این مشکل حتی زمانی که هر سه مدل ممکن است توسط یک شبکه IT واحد ساخته شود، بسیار چالشی تر نیز می شود.

در عین حال، راه هایی وجود دارد که تأثیر روی زیرساخت مجازی نوساز کاربردی خاص را کاهش می دهد.

۳ یک راه حل امنیتی تخصصی برای محیط مجازی لازم است

با اینکه می توان یک عامل امنیتی مورد اعتماد را در نقاط انتهایی ماشین مجازی قرار داد، اما تعداد عمده ای از نارسایی ها وجود دارند که هنوز هم می توانند تجربه مدیر را با زیرساخت IT کمتر راضی کننده نشان دهند.

۱. **نسخه برداری**. هر VM تعداد یکسانی از اجزای امنیتی را به همراه دارد شامل: یک موتور ایزوله ضد بدافزار به همراه پایگاه داده ای از امضای آنها که هر کدام نیاز دارند تا بطور مستقل بروز شوند. بنابراین یک نسبت قابل توجه از منابع با ارزش (توان پردازشی، RAM و disk storage) بسیار بی هدف مصرف شده است که به طور قابل ملاحظه ای نرخ تثبیت نتیجه را کاهش می دهد.

۲. «**طوفان**[۳]». این مورد برای انجام همزمان اسکن ضد بدافزار یا بروزرسانی فعالیت پایگاه داده بوسیله ماشین های چند تایی استفاده میشود که می تواند ناگهان ما را به حالت اوج مصرف منابع و یا حتی

1- Virtual Desktop Infrastructure

[۳] Storms

تا عدم سرویس دهی پیش ببرد. تنظیمات دستی می تواند به حل موقت مشکل بیانجامد اما با تعداد بالای VMها، مداخله دستی هزینه زمانی بسیار سنگینی دارد.

۳. «**شکاف فوری**[۴]». بعضی ماشین های مجازی در حالت به خواب رفته[۵] باقی می مانند تا زمانی که به سرویس فراخوانی شود (در زمان نیاز). متأسفانه امکان بروزرسانی راه حل ها و اعضای امنیتی در زمان خاموش بودن VMمیسر نیست. بنابراین بعد از بالا آمدن و قبل از اتمام بروزرسانی امنیتی، VM به حمله خارجی آسیب پذیر است.

۴. «**حمله وحشتناک**[۶]». این یک عمل متداول است بین مدیران سیستم تا عکس العمل به شیوع یک ویروس را به عنوان محکم کننده پارامترهای امنیتی، از پیش تعریف کنند. مثل رفتن به مد paranoid و شروع کردن یک پروسه برنامه ریزی نشده و این مثل سیاستی که ممکن است برای گره های فیزیکی ارزش داشته باشد، می تواند به سادگی یک محیط مجازی را به یک فضای پر زحمت مبدل کند.

۵. **مشکلات عدم انطباق**[۷]. ماشین های مجازی در بسیاری از موارد مانند همتای فیزیکی خود هستند اما تفاوت های عمده ای وجود دارد که باید آنها را در نظر داشته باشیم، مانند استفاده از دیسک های غیرمداوم یا مهاجرت پروسه از VM روشن و آماده به کار. ضد بدافزارهای استاندارد که برای نود ها پایانی فیزیکی ساخته شده اند، بهایی به بسیاری از خصوصیات ریز محیط های مجازی نمی دهند و بنابراین می تواند باعث ایجاد lagهای غیرمنتظره یا حتی بطور کلی اجرا نشدن بشوند. با توجه به تمام مسائلی که بالا گفته شد، نیاز کلی به یک راه حل اختصاصی، مشخص تر می شود. مثل یک محصول که باید با اگاهی از تمام نکات بالا تولید شود. زمانی که بالاترین مرحله ی ممکن امنیت با کمترین میزان تأثیر روی کل کارایی باید باشد.

---

[۴] Instant-on gap
[۵] Sleep mode
[۶] Panic attacks
[۷] Incompatibility problems

۴ پلت فرم ها و مدل های حفاظت

۴-۱ راهکار فاقد عامل

VMware یکی از قدیمی ترین و هنوز هم یکی از مشهورترین پلت فرم های مجازی سازی است که یک راه حل به نام vShield را فراهم می کند. vShield اجازه می دهد حمل بار یکسانی برای پایگاه داده و دو برابر کننده عامل های ضد بدافزار از عهده[۸] VM برداشته شود. این روش «فاقد عامل» نامیده می شود.

به عنوان مثال Kaspersky Lab یک راه حل امنیتی برای پلت فرم VMwareها ارائه می دهد (Kaspersky Security for Virtualization | Agentless). اینجا اسکن کردن کارها به یک دسته تجهیزات واحد امنیتی مجازی منتقل می شود (SVA[۹])، یک ماشین مجازی مخصوص ـ که هم موتور اسکن و هم پایگاه داده امنیتی را درون خود دارد ـ این ماشین حفاظت کل ماشین های در حال اجرا را تأمین می کند.

فواید این روش این است که:

- رابط بومی که توسط VMware vShield ارائه شده است اجازه دسترسی کارا به ماشین های مجازی را می دهد که امکان آزاد کردن منابع ماشین های تکی و اطمینان از سازگاری آنها با دیگر تکنولوژی های VMware را می دهد.
- منابع به دلیل تمرکز اقدامات ضد بدافزار و نگهداری پایگاه داده امضای آنها روی یک ماشین مجازی واحد که می تواند برای ماشین های مجازی بیشتری هم سرویس دهی امنیتی کند بسیار آزاد شده اند و این باعث افزایش نرخ تثبیت می شود.
- با ورود و بالا آمدن ماشین های جدید، امنیت شان توسط SVA بدون فشار بیش از حد به ماشین یا نیاز به نصب نرم افزارهای اضافه تأمین می شود.
- SVA آماده به کار همیشه پایگاه داده امضاها را مرتباً بروز نگه می دارد.
- مشکل طوفان (Storms) در اینجا بعد از یک به روزرسانی پایگاه داده ریشه کن می شود و SVA به صورت خودکار و طی یک برنامه زمان بندی تصادفی و با اعمال محدودیت در استفاده از نخ، VMها را اسکن می کند.

---

[۸] Virtual Machine

[۹] Security Virtual Appliance

متأسفانه، توانایی های vShield محدود است و تنها امکان اتصال به VMها در سیستم های فایل میسر است. لذا پردازش هایی که در داخل حافظه VM انجام می شوند، قابل کنترل و نظارت توسط «ضد بدافزار فاقد عامل[۱۰]» نیستند. این همچنین به این معنی است که فناوری حفاظت از نقاط دیگر شبکه، مثل کنترل کاربردی دارای لیست سفید پویا که طراحی شده اند تا لایه های امنیتی اضافی شبکه را تأمین کنند، قابل پیاده سازی نیستند.

این باید در نظر گرفته شود که همانطور که vShield به طور اختصاصی یک فناوری مربوط به VMware است، راهکار فاقد عامل هم ـ برای امن کردن یک زیرساخت مجازی ـ در حال حاضر فقط قابل استفاده روی پلت فرم VMware است.

۴-۲ راهکار عامل واسط

با در نظر داشتن محدودیت های ذکر شده در بالا، راهکار دیگری برای مجازی سازی پیشنهاد می شود؛ راهکاری که بین راهکار فاقد عامل و راهکار عامل کامل قرار می گیرد.

همانند راهکار فاقد عامل، پایگاه های داده و موتور اسکن کننده ضد بدافزار روی SVA مستقر هستند. اما یک تفاوت وجود دارد: یک ماژول کوچک و ساکن در هر VM که تحت حفاظت می باشد، بکار گرفته شده است.

مزایای کلیدی راهکار امنیتی ذکر شده در بالا برای مجازی سازی (عامل واسط) عبارتند از:

- مصرف کمتر منابع در مقایسه با راهکار عامل کامل، به دلیل اینکه موتور اسکن سیستم و پایگاه های داده به SVA اختصاصی منتقل شده اند.
- پشتیبانی از محبوب ترین پلت فرم های مجازی سازی ـ VMware، Microsoft Hyper-V و Critix.
- بالاترین سطح حفاظت، ارائه دسترسی کامل به منابع VM از جمله RAM.
- قابل دسترس بودن لایه های امنیتی فعال و اضافی، مانند HIPS مجهز به سیستم جلوگیری از سوءاستفاده خودکار و کنترل کاربردی با لیست سفید سازی پویا. حتی در سخت ترین سناریوهای امنیتی مانند «رد پیش فرض»، به راحتی قابل استفاده است.
- از ابتدا با در نظر گرفتن مجازی سازی طراحی شده، این راهکار با خصوصیات منحصر به فرد محیط مجازی جواب می دهد، نه در برابر آن خصوصیات.

2- Agentless Anti-Malware

اما، هر مسئله ای، بهایی دارد. عامل واسط باید روی هر VM که به تازگی بکار گرفته شده، وجود داشته باشد ـ فرآیندی که از طریق گنجاندن LA[11] در نسخه کپی از قبل تولید شده VM، به راحتی قابل خودکار شدن است. به سبب حضور عامل واسط، در مدل ذکر شده، نسبت به راهکار فاقد عامل، رد بیشتری در حافظه از خود به جای می گذارد؛ ولی شایان ذکر است که تحت شرایط خاص، راهکار عامل واسط در واقع می تواند از راهکار فاقد عامل مبتنی بر vShield پیشی بگیرد.

همچنین تعداد Hypervisor های پشتیبانی شده، محدود به سه پلت فرم رایج است. در زمان انتشار این گزارش، مایکروسافت ویندوز تنها سیستم عامل مهمان بود که از راهکارهای فاقد عامل و عامل واسط پشتیبانی می کرد.

۳-۴ راهکار عامل کامل

امنیت راهکار کامل، با وجود اینکه یک راهکار عامل کامل است، در واقع قادر به انجام فعالیت چشمگیری در محیط های مجازی می باشد.

مزایای استفاده از امنیت راهکار کامل در سرتاسر زیرساخت مجازی عبارتند از:

- پشتیبانی از آخرین سیستم عامل ها.
- اصول مدیریتی کاملاً آشنا، مانند هر ماشین فیزیکی معمولی.
- کارایی آن توسط بزرگترین آژانس های مشاوره تشخیص داده شده (Gartner، IDC و Forrester)، یکی از بهترین پلت فرم های قابل دسترسی حفاظت نهایی نام گذاری شده است.

جدول ۱. لیست خصوصیات نسبی

خصوصیات	امنیت برای مجازی سازی (فاقد عامل)	امنیت برای مجازی سازی (عامل واسط)	امنیت برای مجازی سازی (عامل کامل)
پلت فرم های مجازی سازی پشتیبانی شده	VMware	VMware, Microsoft Hyper-V, Citrix	هر موردی به جز سطح سیستم عامل
سیستم عامل مهمان پشتیبانی شده	مایکروسافت ویندوز	مایکروسافت ویندوز	مایکروسافت ویندوز، Mac OS X و لینوکس
نرخ تثبیت در یک میزبان	***	**/***	*

[11] Light Agent

مدیریت متمرکز از طریق مرکز امنیت متمرکز	+	+	+
قابلیت KSN	+	+	+
حفاظت از VM جدید بدون پیاده سازی های اضافی	+	+/-	-
ضد بدافزار	**	***	***
دیوار آتشین	-	+	+
جلوگیری از نفوذ میزبان محور (HIPS)	-	+	+
مسدودکننده حمله به شبکه	+	+	+
کنترل کاربردی با لیست سفید[۱۲] پویا و پشتیبانی از رد پیش فرض	-	+	+
کنترل وب	-	+	+
کنترل دستگاه	-	+	+
مدیریت سیستم ها	-	+	+
رمزگذاری	-	-	+

بنابراین، پس از انجام تمام محاسبات، مجدداً یک سؤال ایجاد شده: چگونه می توان بیشنه کارایی را بدون آسیب پذیر شدن در مقابل تهدیدات سایبری، به دست آورد؟ روشی وجود دارد که به عنوان حساب سرانگشتی قابل استفاده است و «امنیت مبتنی بر نقش» نام دارد.

۵ فقط دفع حملات ورودی؛ راهکار امنیتی مبتنی بر نقش

تمام نقاط پایانی فیزیکی و تهدیدکننده سایبری نیز می توانند زیرساخت مجازی را تهدید کنند. اما مهاجم به روشی برای نفوذ به محیط امنیتی جهت انجام حمله نیاز دارد. برای مثال، برای آلوده کردن یک کامپیوتر سالم، مجرم سایبری باید کارمند را به سمت وب سایت مخرب ترغیب کند که از طریق سوءاستفاده از یک آسیب

[۱۲] White list

پذیری در مرورگر قربانی، فرآیند آلودگی انجام می شود. ولی برای آلوده کردن یک سرور پایگاه داده که در زیرساخت IT که ممکن است حتی اتصال اینترنت هم نداشته باشد مخفی است، بایستی از روش های دیگری برای حمله استفاده شود. بنابراین، اگر تضمین می گردد که تنها تهدیدات احتمالی، تهدیدات حمله کننده به سطح سیستم فایل، پایگاه داده ای که ارزش کمی دارد یا استفاده از VDI[۱۳] حفاظت شده بدون دسترسی به وب هستند، سازمان می تواند راهکار فاقد عامل را انتخاب کند که مزایای حفاظت فوری و فقدان «شکاف های فوری» را ارائه می کند.

[۱۳] Virtual desktop infrastructure

جدول ۲. راهکار امنیتی مبتنی بر نقش

نقش	دسترسی خارجی	ارزش داده	ارزش سرویس	شرایط اضافی	راهکار (چرا راهکار خاصی استفاده می شود)
سرورهای پایگاه داده Backend	ندارد	کم به متوسط	متوسط به زیاد	پشتیبان گیری معمولی	مرکز مدیریت (فاقد عامل) (داده های دارای طول عمر کوتاه، روش های کم برای حمله)
وب سرورهای Frontend	دارد	کم	زیاد	ارتباطات مطمئن با چندین Backend دارد	مرکز مدیریت (عامل واسط) (در معرض خطرات دسترسی عمومی، پس از حمله موفق، سوءاستفاده از اطمینان نیز امکان پذیر است)
VDI دارای اهداف محدود یا برنامه مجازی سازی شده	ندارد	متوسط به زیاد	متوسط	به شدت محدود، فاقد نصب برنامه، فاقد استفاده از حافظه جداشدنی	مرکز مدیریت (فاقد عامل) (محیط قابل پیش بینی، روش اندک برای حمله)
VDI جایگزین کامپیوتر	دارد	متوسط	متوسط	استفاده از حافظه ذخیره سازی شخصی، کاربران ممتاز دارای امتیازات نصب	مرکز مدیریت (عامل واسط) (نیاز به امنیت بالاتر، نسبت به نیازبه واکنش سریع تر، بیشتر است. روش های بیشتر برای حمله به سبب در معرض اینترنت عمومی قرار داشتن)
وب سرورهای اینترانت سازمانی	دارد	کم به متوسط	کم به متوسط	دسترسی خارجی فقط از کاربران مجاز با استفاده از Tokenهای سخت افزاری	مرکز مدیریت (عامل واسط) (ارزش کم تجاری داده ها، دسترسی بسیار محدود به اینترنت عمومی)
زیرساخت پردازش داده سرویس گیرنده	دارد	زیاد	زیاد	نیاز به محیط ثابت و تغییرناپذیر؛ کنترل کاربردی با رد پیش فرض پیشنهادی	مرکز مدیریت (عامل واسط) (نیاز به انطباق، لایه های امنیتی اضافی را ملزم می کند)
زیرساخت آزمایش توسعه دهندگان وب	دارد	کم به متوسط	متوسط	Hypervisor مبتنی بر لینوکس و VMهای مهمان ناهمگون	KESB برای لینوکس، KESB برای ویندوز (تمدید مداوم داده های دارای طول عمر کوتاه، گوناگونی سیستم عامل ها)

جدول بالا حاوی نمونه هایی است که درک کلی از حفاظت مبتنی بر نقش را ارائه می کند، اگرچه پیشنهاد مستقیمی برای نقش های لیست شده نیست و نباید مورد استفاده قرار گیرند. هر مورد استفاده ای منحصر به فرد است؛ همیشه شرایط بیشتری نسبت به شرایط خلاصه شده در یک جدول وجود دارد که باید در نظر گرفته شوند. با این وجود، برای درک بهتر، طبقه بندی ارزش داده و ارزش سرویس با جزئیات بیشتر ارائه می گردد:

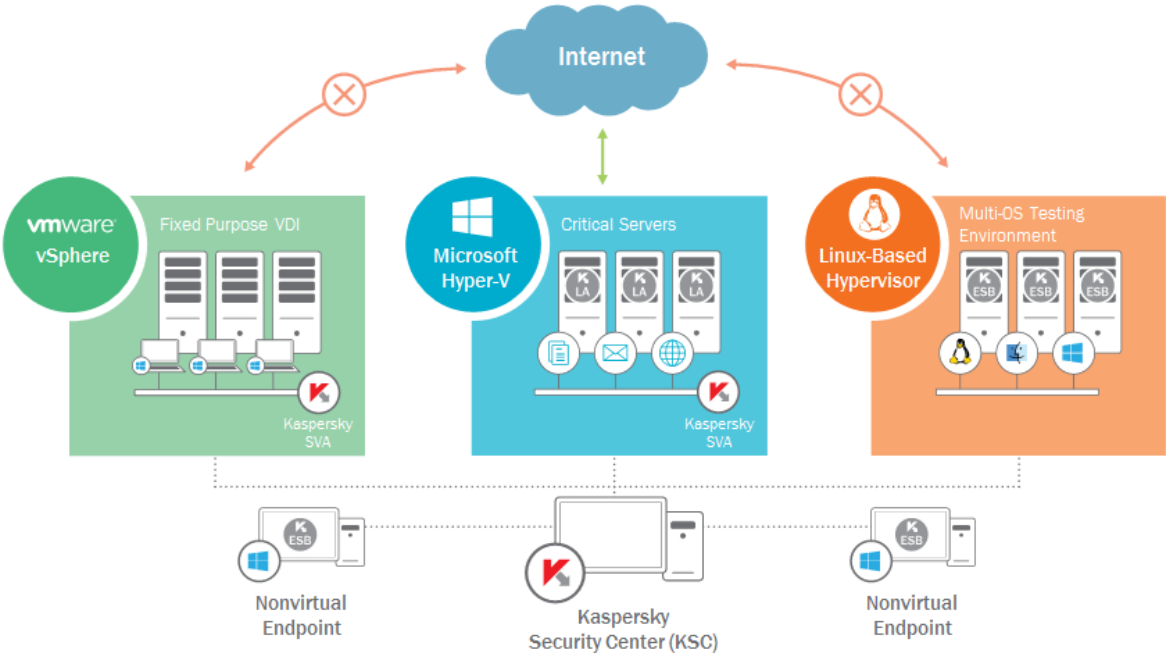
- **داده کم ارزش ـ** این داده معمولاً فاقد شخصیت است، حاوی هیچ گونه اسرار با ارزش شخصی، تجاری یا دولتی نیست و احتمالاً دارای طول عمر کوتاه و در معرض تمدید همیشگی است. از دست رفتن یا افشای آن، منجر به ضررهای تجاری چشمگیری نمی شود و هیچ وقت نمی تواند باعث آسیب به شهرت شود. نمونه ای از آن، پایگاه داده فعال و سالم خواهد بود که داده انتقالی به طور موقت ذخیره می شود.
- **داده دارای ارزش متوسط ـ** این داده می تواند حاوی برخی اطلاعات شخصی یا تجاری به استثنای اتصال مستقیم داده ها به امور مالی و سلامت شخصی باشد. این داده ها حاوی اطلاعات محرمانه نیستند. از دست رفتن آن می تواند باعث آسیب مالی به سازمان شود. افشای آن می تواند منجر به تأثیر قابل توجه مالی شود و قادر به آسیب به شهرت سازمان به شکل غیرحیاتی است. برای مثال، داده های مشتریان متعلق به یک خرده فروش اینترنتی.
- **داده با ارزش ـ** می تواند حاوی اطلاعات حساس شخصی و/یا مالی یا اسرار تجاری باشد که بخش مهمی از سود تجاری سازمان را تشکیل می دهند. می تواند حاوی اطلاعات محرمانه نیز باشد. از دست رفتن آن باعث ضررهای چشمگیر تجاری و اعتباری می شود. افشای آن می تواند منجر به جریمه های سنگین مالی، از جمله شکایات و آسیب قطعی اعتباری، شود. برای مثال، نقشه های زیرساخت حیاتی یا مکاتبات محرمانه در سطح اجرایی.
- **سرویس کم ارزش ـ** هیچ نهاد ثالثی تحت تأثیر قرار نمی گیرد، سرعت بازیابی کم اهمیت است. فاقد پیامدهای مالی یا پیامدهای مالی اندک در صورت خرابی آن. احتمال آسیب اعتباری به شدت پایین است. برای مثال، درگاه اطلاعاتی سازمان.
- **سرویس دارای ارزش متوسط ـ** ممکن است نهادهای ثالث تحت تأثیر قرار گیرند اگر سرویس تخریب شود. از دست رفتن چنین داده هایی می تواند منجر به آسیب چشمگیر مالی شود. آسیب اعتباری نیز چشمگیر است و مستقیماً به اهمیت اجتماعی سرویس ارتباط دارد: هرچه سرویس مشهورتر و محبوب تر باشد (یا محصول متکی به آن)، پیامدهای اعتباری سنگین تر خواهد بود. ممکن است داده ها بخشی از زیرساخت دولتی باشند ولی شرایط آن، تأثیر اندکی روی سلامت کشور دارد. بازیابی سریع، اهمیت ویژه ای دارد. برای مثال، زیرساخت VDI یک فروشنده سیستم، محیط جایگزین کننده کامپیوتر در میان سرویس های آن را فراهم می کند.

- **سرویس با ارزش ـ** نهادهای ثالث، به احتمال قریب به یقین تحت تأثیر هستند. این سرویس، معیار اصلی تجارت است و می تواند معیار حیاتی تجارت های نهادهای ثالث نیز باشد. تأثیر بر سلامت ملی نیز امکان پذیر است. ضررهای اعتباری بسیار زیاد هستند و ممکن است قطعی باشند. بازیابی، بیشترین اهمیت را دارد؛ ناتوانی در انجام بازیابی موفق در کوتاه زمان، می تواند باعث پیامدهای عمده تری شود. برای مثال، زیرساخت سیستم کنترل ویدیویی دولت.

هر فردی زیرساخت خود را بهتر می شناسد، بنابراین می تواند بهترین تصمیم را درباره امنیت خود بگیرد؛ دستورالعمل های ارائه شده در این گزارش، اصول پایه برای تصمیم گیری هستند. ولی، امکان تقویت کارایی بهره برداری از منابع و ذخیره سرمایه برای شرکت و در عین حال ایمن نگه داشتن زیرساخت مجازی، کاملاً وجود دارد. بایستی به خاطر داشت که قبل از بکارگیری هر گونه راهکار امنیتی تخصصی، بایستی تنظیمات پایه امنیتی شبکه IT بررسی و تعدیل شوند. شبکه مدیریت شده، به معنی روش های کمتر حمله برای مجرمان و جمع آوری پیامدهای کمتر برای سازمان در صورت بروز خطا، است.

۶ کارایی یعنی تمامیت

استفاده بهینه از منابع بسیار عالی است ولی بدون کنترل مؤثر، کاربری مناسبی ندارد. سازمان قطعاً می تواند راهکار فاقد عامل را برای Back-endهای یک فروشنده، راهکار عامل واسط برای VDI از فروشنده دیگری بکار گرفته و کنترل کاربردی ثالث را برای نواحی حیاتی اضافه کند. در نتیجه، سه کنسول مدیریت و سه مجموعه سیاست به منظور پیکربندی و نگه داری و ترافیک بسیار زیاد به روزرسانی جهت تزریق از طریق کانال داده وجود دارد. مطمئناً بکارگرفتن تمام موارد از یک فروشنده که تمام تنظیمات و کنترل ها به طور صحیح درون یک کنسول سازمان دهی شده باشند، بسیار بهتر است.



شکل ۱. محیط شامل چند Hypervisor می تواند به شدت و به طور مؤثر حفاظت شده باشد

برای مثال، هسته Active Directory (کنترلرهای دامنه، سیستم های نام دامنه و غیره) می تواند روی سرورهای مجازی Microsoft Hyper-V میزبانی شده، یک VDI مبتنی بر Citrix استفاده شده و حاوی چندین سرور پایگاه داده که روی VMware ESXi اجرا می شوند نیز باشد. همان طور که در تصویر بالا نشان داده شد، سازمان می تواند یک محیط ترکیبی حاوی چندین پلت فرم Hypervisor و همچنین نقاط پایانی فیزیکی را اداره کند.

در این مورد، برای مؤثرترین عملکرد/توازن امنیتی که منجر به نرخ های بهینه تثبیت می شود:

- VDI مجزا و تک منظوره می تواند از طریق مرکز مدیریت (فاقد عامل) محافظت شود.
- زیرساخت سروری که برای تجارت حیاتی است و حاوی داده های باارزش می باشد، باید از طریق لایه های امنیتی قدرتمند حفاظت شود.

- محیط آزمایش حاوی Hypervisor لینوکس و تعداد زیادی سیستم عامل های مهمان و همچنین نقاط پایانی فیزیکی، به بهترین شکل ممکن محافظت شده است.

۷ اشتباهات امنیتی که در مجازی سازی

استفاده از فناوری مجازی سازی با فایده های زیادی مانند زیرکی و چالاکی و انعطاف پذیری صرفه‌ی اقتصادی همراه است. در عین حال آشنایی با مجازی سازی ما را با چالش هایی نیز اشنا می‌کند:

- یک شبکه ی مجازی جدید معمولا نسبت به دستگاه های امنیتی فیزیکی دیدی ندارد.
- یک سطح تهدید جدید: hypervisor
- یک مدیر توانمند در حوزه ی مجازی که با خود به هم ریختگی پست ها را به همراه دارد.
- ماشین های سیار: احتمال سرقت

در کنار فواید بسیار زیاد مجازی سازی، تهدیدهای بسیاری نیز بصورت خود ساخته وجود دارند. بدلیل کمبود اطلاعات و راهنمایی های مناسب برای استفاده از مجازی سازی و ماشین های مجازی، کارمندان اشتباهات حساس زیادی را مرتکب می شوند که برای سازمان و امنیت مجازی سازی بسیار خطرناک است.

متخصصین حوزه امنیت نیاز دارند تا چیز های جدید را تشخیص دهند و توانایی های امنیتی خود را با آن ها تطبیق دهند. در غیر این صورت مجازی سازی یک ریسک جدی امنیتی نشان داده می شود. همانطور که ماشین های مجازی جدید مدام روی خط تولید می روند، سازمان ها نیز بدرستی در مورد فناوری استفاده شده در ماشین های مجازی احساس خطری از راه های جدید علیه خودشان دارند.

با اینکه راه حل های زیاد امنیتی برای امن کردن یک سازمان وجود دارد اما هنوز هم آگاهی کارمندان و استفاده امن از سرور ها و ماشین های مجازی نقش مهمی را ایفا می کنند. به علاوه ی این نگرانی ها مشکلی که رتبه ی نخست را درمیان مشکلات مجازی سازی داراست ، اشتباهاتی است که کاربران و مدیران در حین استفاده و تنظیم ماشین های مجازی مرتکب می شوند که به نحوی تاثیراتی بر جنبه های امنیتی مجازی سازی دارد.

۷-۱ اشتباهات مدیریتی در مجازی سازی

اشتباه اول: عدم پیکربندی سطوح میزبان، مهمان و شبکه

پیکربندی امنیتی ماشین های مجازی عملا مثل پیکربندی به صورت پیشفرض ماشین های فیزیکی است با این تفاوت که در سرورهای مجازی این بزرگترین اشتباهی است که مدیر یک ماشین مجازی می تواند انجام دهد.

اگر شروع ساخت یک ماشین با پیکربندی پیش فرض ضعیف انجام شود -شامل پورت ها و سرویس ها و... غیر ضروری- آسیب پذیری ها به هر نمونه از آن ماشین مجازی ساخته شده سرایت خواهند کرد.

پیکربندی شبکه های مجازی نیز حوزه ی دیگری است که سازمان ها در ان اشتباه میکنند. در یک شبکه ی مجازی بعضی سازمان ها هنوز هم وب سرور و پایگاه داده را بدون دسته بندی مناسب میزبان قرار می دهند.

این اشتباهات ساده میتواند سرور مجازی را به راحتی به هدفی برای حمله ی هکر ها تبدیل کند تا در سرور و دیگر سرویس ها رخنه کنند.

برای جلوگیری از این اشتباه تمام سیستم های مانیتورینگ باید اگاه از ماشین های مجازی باشند و باید قابلیت تشخیص و عمل را با توجه به مورد داشته باشد. باید بتوانند دقیقا تمام سازگاری های سطح مجازی سازی که ارتباط بین سیستم عامل های مهمان و میزبان را برقرار میکند بررسی کنند. مانند: درایور دستگاه ها، عملیات های copy و paste ، انتشار ناخواسته قسمت هایی از حافظه و دیگر موارد. جایی که امکان دارد این قابلیت ها باید شناسایی و غیر فعال شوند.

اشتباه دوم: ناکامی در تقسیم مناسب وظایف و گسترش حداقلی امتیازات کنترلی

در هر سازمانی، امتیازات کنترلی نقش مهمی را بازی می کند. مهاجمان همیشه به دنبال اتصال پیدا کردن به حساب های کاربری امتیاز دهی شده اند تا بتوانند سرور ها را نابود کنند. در مجازی سازی، این یک اشتباه رایج است که حساب های کاربری امتیاز دهی شده را از سایر حساب ها جدا و پشتیبانی نشده رها کنند.

تقسیم مشخص وظایف و دادن کمترین امتیازات ضروری به کاربران برای انجام کارهای امن شده در هر دو منابع مجازی و فیزیکی حیاتی هستند.

بعضی سطوح مجازی سازی کارایی های سیستم و مدیریت شبکه را از کار می اندازد. بطوری که این گونه تقسیم وظایف، سخت می شود. این سطوح، امتیازیات و سازگاری های زیادی را به مدیران می دهند.

علاوه بر این، اتصالات با امتیازات بالا میزان ریسک سوءاستفاده توسط کارمندان داخلی را نیز افزایش میدهد. فراتر از مشکل افراد داخلی ، سازش با گواهی های ورود مدیران هم می تواند مهاجمان را با مجموعه ای از امکانات قوی برای حمله ای بیرونی روبرو کند.

برای جلوگیری از این اشتباه بحرانی، باید از قوانین فیلترهای دیواره ی آتش استفاده کرد تا کنسول مجازی اتصال مدیران به آدرس های شبکه ی از پیش تعیین شده و مجوز داده شده ی داخلی را محدود کرد، با این کار می توان با مهاجم خارجی که برای که اتصال به کنسول مجازی مدیر آمده مقابله کرد. علاوه بر این استفاده از مکانیزم های مورد اعتماد امنیتی مانند درخواست SSH برای اتصال به کنسول مدیر را باید در نظر داشت.

اشتباه سوم: ناکامی در تربیت گروه های دیگر ، به خصوص مدیریت ریسک و تطبیق کارکنان

ارزیابی ریسک، تطبیق و حتی قرارداد نرم افزاری زمانی که ماشین های مجازی می توانند بطور پویا برپا شوند، به خواب بروند یا از بین بروند، تحت فشار قرار میگیرند.

روش های سنتی برای ارزیابی ریسک و آنالیز (ارسال پرسشنامه های ارزیابی، آنالیز جوابها) شاید در محیطی مجازی کافی نباشد. تعداد زیادی از سازمان ها در انالیز شکاف ها به دلیل دیدگاه اشتباه در محیط چند ریسکی شکست خورده اند.

می توان با تدریس مدیریت ریسک و تربیت گروه های انطباقی درباره ی قابلیت ها و محدودیت های مجازی سازی، جلوی این مشکل را بگیریم.

اشتباه چهارم: کم تر دیده شدن VM در جامعه سرمایه گذاری

انتشار سیستم های مجازی در جامعه سرمایه گذاری در یک راه کنترل نشده، اشتباه عمده ی یک سازمان است که روی اکثر سیستم ها مکانیزم های مجازی تاثیر گذار است.

یک مدت معمول پراکندکی VM برای تعریف کردن چنین انتشارات کنترل نشده ای استفاده می شود. این به ماشین ها اجازه می دهد تا منابع و پهنای باند را طوری استفاده کنند که اسیب پذیری های جدیدی در ماشین های مجازی رونمایی شوند که نه اضافه و نه مانیتور شده اند.

بطور کلی کشف سیستم های مجازی (و کاربرد های قابل اجرا روی انها) کاری مهم و چالش برانگیز است. به این علت است که دید داشتن در محیط مجازی بسیار مهم است.

در هر حادثه ای زمانی که قوانین انجام می شوند، محیط مجازی در تاریکی دید باقی می ماند که به علت اشتباهاتی از این قبیل است و یک مشکل تمام عیار را در زمان از دست دادن اطلاعات موجود روی منابع ناشناخته و نا امن مجازی ایجاد خواهد کرد.

۲-۷ اشتباهات فنی در مجازی سازی

اشتباه اول: مجازی سازی سخت افزارهای قدیمی: هم Microsoft Hyper-V و هم VMware سرور می توانند روی سخت افزارهای قدیمی اجرا شوند. با این حال پردازنده های جدیدتر قابلیت هایی ماند SLAT[۱۴] و NPT دارند که به مقدار خوبی باعث افزایش کارآیی مجازی می شود. این کار با اجازه دادن به سخت افزار برای انجام کارهای تبدیل بین آدرس حافظه ای ماشین مجازی مهمان و آدرس های فیزیکی RAM انجام می‌شود. این قابلیت ها همچنین باعث می شوند تا تبدیل آدرس به حالت سخت افزاری تغییر یابد که امنیت بیشتری در پی خواهد داشت.

اشتباه دوم: اجرای آنتی ویروس روی هارد دیسک های مجازی: استفاده از آنتی ویروس همیشه فکر خوبی است ولی اسکن کردن هارد دیسک های مجازی توسط آنتی ویروس می تواند باعث کاهش کارآیی VM شود. مطمئن باشید که هارد دیسک های مجازی را از اسکن آنتی ویروس میزبان خارج کرده اید. در این صورت برای حفظ امنیت استفاده از آنتی ویروس ها در داخل ماشین مجازی ضروری است.

اشتباه سوم: نادیده گرفتن تهیه نسخه پشتیبان VM مهمان: شما می توانید از VM روی ماشین میزبان بدون اینکه کارهای کاربر با وقفه مواجه شود بک آپ بگیرید. با این کار عملیات ریکاوری را راحت تر کرده اید. چون می توانید این بک آپ را در عرض چند دقیقه روی یک VM دیگر نصب کنید. با این حال، بک آپ های سطح میزبان نمی‌توانند به عنوان جایگزین بک آپ های مهمان شوند. برنامه هایی مانند Microsoft و Sharepoint نیاز دارند که برای محافظت از اطلاعات کاربران در سطح مهمان از آنها بک آپ گرفته شود. امروزه به دلیل رشد باج افزار ها که عمدتا فایل های کاربران را رمز می کنند نسخه های پشتیبان در سطح میزبان ضروری است.

[۱۴] Second Level Address Translation

اشتباه چهارم: امنیت پایین میزبان: ایمن کردن ماشین مهمان بدون در نظر داشتن ایمنی ماشین میزبان زیاد اتفاق می افتد. در حالی که امنیت ماشین میزبان به دلیل داشتن دسترسی به اطلاعات مهمان مهم تر است. میزبان باید دارای امنیت فیزیکی باشد و تمام منابع روی میزبان باید با توجه به سطح دسترسی امنیت داشته باشند.

اشتباه پنجم: استفاده از تنظیمات پیش فرض VM: یکی دیگر از اشتباهات رایج استفاده‌ی کورکورانه از تنظیمات اولیه‌ی میزبان روی کنسول مدیریت VM است. علاوه بر این، کارشناس پیاده سازی مجازی باید به مقدار CPU، RAM، دیسک و شبکه‌ی هر VM توجه داشته باشد تا با میزان مورد نیاز VM هم خوانی داشته باشد.

اشتباه ششم: منابع پردازشی میزبان ناکافی: مجازی سازی به شما اجازه می دهد استفاده‌ی بیشتری از سخت افزار نسبت به یک سرور فیزیکی ببرید. با این حال چیزی نمی تواند مانع از استفاده‌ی بیش از حد از CPU میزبان شما با نصب تعداد زیادی VM روی آن شود. در حالت عادی باید به ازای هر VM یک هسته‌ی CPU داشته باشید. بخش Windows Server Resource Monitor می تواند اطلاعاتی راجع CPU و استفاده از هسته های آن را به شما بدهد. همچنین باید توجه داشت که حداکثر میزان پردازش یک ماشین مجازی در کار ماشین میزبان اختلالی ایجاد نکند. در غیر اینصورت یک حمله DDoS به ماشین مجازی می تواند منجر به اختلال در میزبان نیز بشود.

اشتباه هفتم: میزان ناکافی RAM: کمبود RAM قطعاً تأثیر زیادی روی محیط شبیه سازی شده‌ی شما می گذارد (حتی بیشتر از کمبود CPU). RAM اولین فاکتور محدود کننده تعداد VM های فعال به طور همزمان روی یک میزبان است. به این دلیل که هر VM باید میزان حافظه‌ی درخواستی خود را مستقیماً از حافظه‌ی فیزیکی بگیرد. باید مطمئن شد که میزان RAM میزبان به اندازه‌ی کافی برای تعداد VM هایی که می خواهند اجرا شوند و همینطور مقداری RAM برای خود میزبان وجود دارد.

اشتباه هشتم: کارت آداپتورهای شبکه‌ی میزبان به مقدار ناکافی: یک اشتباه رایج دیگر – به ویژه در پروژه های مرتبط با سرور- عدم نصب تعداد کافی کارت های آداپتور شبکه بر روی میزبان است. در یک محیط تثبیت سرور، تمام پهنای باندی که از سمت VM درخواست داده می شود از طریق آداپتورهای شبکه‌ی میزبان درخواست داده می شود. با این که ممکن است یک ارتباط یک به یک نیاز نداشته باشید این که تعداد کمی

آداپتور شبکه توسط تعداد زیادی VM مورد استفاده‌ی بیش از حد قرار بگیرند بسیار است. همچنین باید در پیکربندی صحیح آداپتورهای شبکه دقت کرد تا شبکه هر ماشین مجازی به صورت ایزوله نسبت به بقیه ماشین ها و میزبان باشد. در غیر اینصورت ترافیک آلوده می تواند به دیگر قسمت های سرور نیز وارد شود.

اشتباه نهم: تعداد زیادی VM به ازای Volume به اشتراک گذاشته شده: CSV[۱۵] ها یک قابلیت جدید در Windows Server 2008 است که اجازه می دهد چند VM یک LUN را به اشتراک بگذارند. به صورت پیش فرض، تمام VM ها به سمت یک CSV می روند. این طراحی می تواند برای محیط های کاری سبک مناسب باشد ولی محیط های سنگین تر مانند SQL server نیاز به CSV های بیشتر دارند. علاوه بر این، به یاد داشته باشید که کارآیی دیسک بستگی به تعداد حلقه های آن دارد. پس از استفاده از حافظه ای با تعداد حلقه های بیشتر کارآیی بیشتری دارد.

اشتباه دهم: فکر کردن به این که می توان فقط یک CSV به ازای هر VM استفاده کرد: خیلی از توسعه دهندگان فکر کنند هر CSV را فقط برای یک VM می توان استفاده کرد. نه تنها می توان بیش از یک CSV به ازای هر سرور مجازی ایجاد کرد، بلکه می توان VHD فایل های VM ها را بین CSV های مختلف پخش کرد. مدیر سرور می تواند سیستم فایل ها و صفحه‌ی فایل را روی یک VHD بر روی یک CSV پخش کرده و فایل یک VHD روی CSV دیگری قرار دهد.

[۱۵] Cluster Shared Volume

۸ منابع

- http://resources.infosecinstitute.com/security-mistakes-avoid-virtualization/
- http://windowsitpro.com/virtualization/top-ten-virtualization-mistakes
- http://media.kaspersky.com/en/business-security/Virtualization-Understand-the-Difference.pdf