امنیت vSphere

برای متخصصان امنیت، مدیران و کارشناسان زیرساخت مجازی سازی

ترجمه و تألیف:

مهندس روزبه نوروزی

CISSP, PMP

مهندس [illegible] واشقانی فراهانی

کارشناسی ارشد مهندسی شبکه‌های کامپیوتری

کاری از: گروه آموزشی پژوهشی روزبه

مشاوره و آموزش تخصصی فناوری و امنیت اطلاعات

NAGHOOS PUBLICATION

۱۳۹۷

سرشناسه : نوروزی،روزبه،۱۳۵۷-
عنوان و نام پدیدآور : امنیت vSphere برای متخصصان امنیت، مدیران و کارشناسان زیر ساخت مجازی سازی/ ترجمه و تالیف روزبه نوروزی،فرزانه واشقی فراهانی(کاری ازگروه آموزشی پژوهی روزبه)
مشخصات نشر : انتشارات ناقوس-۱۳۹۷
مشخصات ظاهری : ۳۷۰ص.:مصور،جدول،نمودار.
شابک : 978-600-473-118-8
وضعیت فهرست‌نویسی : فیپا
موضوع : وی‌ام‌ویر وی اسفر
موضوع : VMware vSphere
موضوع : کامپیوترها--سیستم های مجازی
موضوع : Virtual computersystems
شناسه افزوده : واشقی فراهانی،فرزانه،۱۳۷۰-
رده بندی کنگره : ۱۳۹۷ ۹ن۹و/QA ۷۶/۹
رده بندی دیویی : ۰۰۵/۴۳۶
شماره کتابشناسی ملی : ۵۱۵۱۹۳۸

انتشارات ناقوس

نام کتاب : امنیت vSphere برای متخصصان امنیت، مدیران و کارشناسان زیر ساخت مجازی سازی
ناشر : انتشارات ناقوس
ترجمه و تالیف : روزبه نوروزی ، فرزانه واشقی فراهانی
چاپ اول : ۱۳۹۷
تیراژ : ۱۰۰
قیمت با یک عدد DVD : ۶۵۰۰۰۰ ریال
چاپ و صحافی : نارنجستان
شابک : ۹۷۸-۶۰۰-۴۷۳-۱۱۸-۸
ISBN : 978-600-473-118-8

مرکز پخش: انتشارات ناقوس
۱-بلوار کشاورز-خیابان ۱۶آذر-کوچه پارسی پلاک ۱۰
تلفن و فاکس : ۶۶۴۷۸۹۵۱- ۶۶۴۷۸۹۵۴

مقدمه مولف:

کتابی مورد نیاز کتابخانه هر سازمان IT محور:

زیرساخت های فناوری اطلاعات بار بزرگی از خدمات IT را به دوش میکشند و به نوعی نقش تعیین کننده ای در پیشرفت و توسعه سازمان دارند . تمامی سرویس ها فضای سایبری درصورتی موفق خواهند بود که برروی زیرساختی قابل اعتماد و پایدار بنا شده باشند .زیرساخت های فناوری اطلاعات چون برق برای کشور هستند که نبود یا خلل در آن ، بسیاری از فعالیت های کشور در روزگار امروز را بی معنا میکند .انتخاب هادر حوزه زیرساخت های فناوری اطلاعات بایستی با دید باز و پس از بررسی اثرات مترتب و ابعاد آن انجام شوند . از سویی هر گاه فناوری در زیرساخت ها استفاده شد بایستی با کلیه جنبه های آن بکار گرفته شوند. برای مثال استفاده از زیرساخت مجازی بدونه درنظر گرفتن امنیت مورد نیاز، باعث شده است علی رغم مزایای فراوان این زیرساخت ، برخی از سروس دهندگان تلاش کنند که به سرر های فیزیکی مهاجرت کنند!! که تعجب بر انگیز است ولی در نظر نگرفتن پیاده سازی زیرساخت مجازی با تمامی خصوصیات و ملزومات آن ، مالک سرویس را نسبت به آن بی اعتماد کرده است.

مثالی دیگر از این دست را میتوان اتخاذ فناوری های SDN (برای نمونه NSX)نام برد . تا زمانی که سازمان ارزیابی درستی از نقاط قوت و ضعف این فناوری ندارد و آنرا با رقبا مقایسه نکرده است نمیتواند قدمی برای اجرای آن بردارد . بله درست است NSX در مقوله امنیت بسیار خوب عمل میکند اما اثرات نامطلوب آن در صورت استفاده نابجا و نابهنگام بسیار خطرناک است و میتواند برخی نفوذ های امنیتی را موجب شود که هیچ گاه قابل کشف نباشند. در خصوص امنیت vSphere نبایستی دیدگاهمان جهت گیری شده به پیاده سازی NSX باشد چرا که محل اعرابی از NSX برای امن سازی در این خصوص وجود ندارد . همانطور که شرکت معظم VMware مستند قابل توجهی برای امن سازی این زیرساخت بدونه توجه به NSX داده است دیده میشود امن سازی vSphere جدای مقوله NSX است . تا زمانی که زیرساخت امن نداشته باشید و طراحی آن بصورت امن انجام نشده باشد امکان مقابله با بدخواهان و هکر ها و اصولا کشف نفوذ و تلاشهای کارشناسان SOC هم بی معنا است . طراحی

زیرساخت امن نیازمند دید همه جانبه و عمیق در طراحی زیرساخت، فراهم آوری طرح شبکه قابل دفاع، با دید بالا است.

نکته آخر که باید یادآور شدآن است که امن سازی زیرساخت مجازی یا هر زیرساختی برخلاف تصور متخصصان معمول امنیت ، با برآورده کردن خواست های یکسری چک لیست های مقاوم سازی حاصل نمیشود . چک لیست ها برای کنترل تنظیمات، بصورت امن هستن ولی اگر ما کلا از پایه امنیت را در vSphere در نظر نگرفته ایم نبایستی برای امنیت به Hardening اکتفا کنیم . بنا بر این اصل و مشاهده این خلاء امنیتی بزرگ در کشور و برای کمک به امن سازی زیرساخت های مهم کشور و ارتقای دانش این مرز و بوم و سازمانها تصمیم گرفته شد کتابی در حوزه امنیت vSphere توسط گروه آموزشی پژوهشی روزبه (در راستای رسالت تاسیس آن) به رشته تحریردرآید.

در ترجمه کتاب سعی شده است از واژگان فارسی استفاده شود و همانگونه که میدانیم این موضوع ممکن است در برخی موارد درک معنا را مشکل کند .لذا سعی شده است در مواقعی که جملات غامض شده اند یا بازنویس موضوع برطرف شده است یا به ناچار از واژه یا واژه های انگلیسی عینا استفاده شده است

نکته مهم در این بین آن است که با توجه به سطح بالای مفاهیم این مستند لازم است پیاده کننده آن چند نکته را مد نظر داشته باشد

۱. خود او از دانش امنیتی پایه در حد SSCP برخوردار باشد یا امور را با کمک یه همراه با تخصص امنیت پیش ببرد
۲. تسلط نسبی به کلیه مقولات مجازی سازی مهم به نظر میرسد چه کارد اطات دانشی فیمابین امنیت و خود موضوع نیازمند سطح دانش و تجربه در حد مناسبی است تا نتیجه مطلوب حاصل گردد.

شایان ذکر است گروه آموزشی پژوهشی روزبه و شرکت امن گستران روزبه با دراختیار داشتن کارشناسان مسلط در حوزه مجازی سازی و امنیت، آماده ارایه خدمات کامل در این حوزه است . ضمنا درصورت نیاز به آموزش امن سازی vSphere و سایر محصولات VMware و دوره های تخصصی امنیت اطلاعات میتوانید با آکادمی آموزش روزبه در آدرس های ذیل تماس حاصل نمایید.

با توجه به وسعت استفاده از vSphere وجود این کتاب در کتابخانه هر سازمان و رجوع مکرر به آن اجباری مینماید . در این میان سعی داریم با همت دلسوزان این مرز و بوم در کاری مشترک ، تلاشهایی برای ارتقای امنیت زیرساخت مجازی کشور برداشته شود در همین

رابطه سایت www.VMwaresecurity.ir برای ای نشر و اشتراک دانش در حوزه امنیت محصولات VMware به همراه فروم های لازم ایجاد میگردد.

لازم است از دقت و پیگیری در خور توجه سرکار خانم فرزانه واشقانی فراهانی برای ارایه بهینه این کتاب ، حمایتهای جناب آقای ترک تبریزی مدیر امور فناوری اطلاعات بانک ملت در راستای پیاده سازی سیاستها و طرح های امنیتی در آن بانک، راهنمایی های جناب آقایان مهرداد توکلی و نوید برادران اساتید مجازی سازی، و پیگیری های جناب آقای محمد حمایتی عدل در خصوص چاپ بهینه کتاب قدردانی گردد. ضمنا تشکر فراوان خدمت جناب آقای اکبری شمیرانی مدیرکل امنیت بانک ملت تقدیم میگردد چراکه اراده راسخ ایشان در پیاده سازی امنیت بصورت علمی و پیگیری راهکارهای اجرایی و اصولا تعهد ایشان به امنیت (Management Commitment)، مثال زدنی است .ضمنا در صورت وجود نظر در خصوص کتاب یا وجود اشکال درآن ،صمیمانه خواهشمند است با ما مدیر کانال تلگرامی گروه منعکس شود.

روزبه نوروزی

CISSP , PMP

مدیر و موسس گروه آموزشی پژوهشی روزبه

مشاوره و آموزش فناوری و امنیت اطلاعات

www.roozbehgroup.com

راههای ارتباطی

آدرس کانال تلگرامی آموزش Https://t.me/roozbeh_learning

www.Roozbeh.Academy

آدرس وبسایت آکادمی آموزش روزبه، مجری تخصصی دوره های امنیت اطلاعات

www.CISSP-Iran.com نقطه ارتباطی شما با مدرک عالی امنیت اطلاعات

www.vmwaresecurity.irآموزش و پژوهش در خصوص مجازی سازی

فهرست مطالب

فصل اول: امنیت اطلاعات و فضای سایبری امروزه

فصل دوم: امنیت در محیط vsphere

فصل سوم: مجوزها در vsphere و وظایف مدیریت کاربر

فصل چهارم: امن‌سازی میزبان‌های ESXi

فصل پنجم: امن‌سازی سیستم‌های سرور vCenter

فصل ششم: امن‌سازی ماشین‌های مجازی

فصل هفتم: رمزگذاری ماشین مجازی

فصل هشتم: استفاده از رمزگذاری در محیط vSphere

فصل نهم: امن‌سازی شبکه vSphere

فصل دهم: روش‌های اشتراکی بین چند عنصر از vSphere

فصل یازدهم: مدیریت پروتکل TLS

فصل دوازدهم: حقوق تعیین شده

فصل سیزدهم: تغییرات نسخه ۶.۷ درحوزه امنیت

منابع