

امنیت رایانش ابری

تهدیدات، چالش‌ها، معماری امنیتی و استانداردها

تالیف:

دکتر احمد صلاحی

آراد کتاب

عنوان و پدیدآور	: امنیت رایانش ابری، تهدیدات، چالش‌ها، معماری امنیتی و استانداردها /
تألیف احمد صلاحی	
مشخصات نشر	: تهران، آراد کتاب، ۱۳۹۶
مشخصات ظاهری	: ۲۳۰ ص، مصور.
شابک	: ۹۷۸-۶۰۰-۱۸۶-۳۳۹-۴
موضوع	: محاسبات ابری
موضوع	: محاسبات ابری - تدابیر ایمنی
رده بندی کنگره	: ۱۳۹۶ الف۸ص/۵۸۵/ QA ۷۶
رده بندی دیویی	: ۰۰۴ / ۶۷۸۲
شماره کتابخانه ملی	: ۴۹۲۷۹۳۷

امنیت رایانش ابری

تهدیدات، چالش‌ها، معماری امنیتی و استانداردها

تألیف: دکتر احمد صلاحی	ناشر: آراد کتاب
نوبت چاپ: اول	
سال چاپ: ۱۳۹۶	تیراژ: ۵۰۰ جلد
چاپ و صحافی: مهرگان	قیمت: ۲۳۵۰۰۰ تومان
شابک: ۹۷۸-۶۰۰-۱۸۶-۳۳۹-۴	

حق چاپ برای پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) با عنایت به قانون حمایت مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸ محفوظ است و متخلفین تحت پیگرد قانون قرار می گیرند.

با همکاری و حمایت پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

مرکز پخش و فروش:

انتشارات آراد کتاب تلفن: ۰۹۱۲۳۰۶۲۴۵۸ - ۶۶۴۸۲۲۲۶ - ۶۶۹۷۵۲۸۵

فروشگاه اینترنتی: www.aradbook.com

پیشگفتار

با تمام مزایای رایانش ابری و توان بالقوه آن برای کاهش هزینه و کاستن زمان لازم برای شروع طرح‌های جدید بدون سرمایه‌گذاری برای ایجاد زیرساخت‌های لازم برای آن طرح‌ها و استفاده از نرم‌افزارها، سخت‌افزارها و سرویس‌های تست شده و قابل اطمینان که به وسیله آنها می‌توان سرویس‌های جدید ایجاد نمود و کشسانی در مقیاس و اندازه امکانات ارائه شده به وسیله ارائه‌دهندگان خدمات ابری، امنیت رایانش ابری همواره یک نگرانی عمده برای کلیه بازیگران رایانش ابری بوده است، شناخت تهدیدات و چالش‌های امنیتی می‌تواند به طراحی معماری امنیتی مناسب برای رایانش ابری جهت جلوگیری و یا کاهش اثرات حملات کمک نماید.

محتویات این کتاب که ساماندهی مجموعه‌ای از داده‌های علمی از منابع مختلف می‌باشد به سه موضوع مهم در امنیت رایانش ابری یعنی، چالش‌ها و تهدیدات امنیتی، معماری امنیتی و استانداردهای رایانش ابری می‌پردازد.

بخش اول کتاب مفاهیم مورد نیاز رایانش ابری را از منابع [1] و [2] نقل می‌نماید تا تعریف دقیقی از رایانش ابری و معماری آن شامل بازیگران، مدل بکارگیری و خدمات ابری ارائه شود. بخش دوم کتاب ترجمه و تلخیص [3] است و یک چارچوب امنیتی برای رایانش ابری جهت تجزیه تحلیل تهدیدات و چالش‌های امنیتی در محیط رایانش ابری و قابلیت‌های امنیتی که می‌توانند آثار این تهدیدات را کاهش داده و با چالش‌های امنیتی مقابله کنند را توصیف می‌کند و یک روش چارچوب برای تعیین اینکه کدامیک از این قابلیت‌های امنیتی نیاز به مشخصاتی برای کاهش تهدیدات امنیتی و مقابله با چالش‌های امنیتی در رایانش ابری دارند را ارائه می‌کند.

معماری امنیتی رایانش ابری در بخش سوم با توجه به منابع [4 و 2] به صورت مشروح ارائه شده است و در آن رایانش ابری مورد اعتماد، ارتباطات و محیط اجرایی امن، مدیریت شناسه و کنترل دسترسی، امنیت خودکار بحث می‌شود. معماری امنیتی رایانش ابری یک عنصر حیاتی در ایجاد اطمینان در الگو و نمونه رایانش ابری است. اطمینان در استفاده از ابر بسته به مکانیسم‌های محاسباتی قابل اعتماد مدیریت شناسه قوی و تکنیک‌های کنترل دسترسی است که محیط اجرایی امن، ارتباطات ابری امن و ریز معماری پشتیبانی کننده‌ای را ارائه دهند. محاسبات خودکار می‌تواند خودمدیریتی، خودبهبوددهندگی، تکنیک‌های خودحفاظتی را برای ساختن رایانش ابری قابل اتکاءتر، امن‌تر و انتخاب سالم‌تر برای الزامات رو به رشد پردازش و ذخیره‌سازی حجم عظیم اطلاعات به صورت مقرون به صرفه ارائه نماید. در بخش چهارم کتاب

امنیت برنامه‌های کاربردی و داده‌های مبتنی بر ابر یکی از نگرانی‌های عمده مشتریان ابری است. نرم افزار امن و مدیریت چرخه عمر نرم افزار امن در حفاظت خدمات ابری امری ذاتی و طبیعی است. امنیت اطلاعات سیستم‌های ابری وابسته به اصول کلاسیک محرمانگی، دسترس پذیری و یکپارچگی است که در معماری‌های توزیع شده، مجازی‌سازی شده و پویا به کار گرفته می‌شوند. اصول مهم به کارگیری و طراحی نرم افزار امن شامل کمترین امتیاز دهی، جداسازی وظایف، دفاع در عمق، امن بودن نسبت به خرابی و طراحی باز می‌باشد.

نرم افزار ابر امن همچنین وابسته به بکارگیری مهندسی الزامات نرم افزار، اصول طراحی، شیوه‌های برنامه نویسی، پیاده سازی سیاست امنیتی و تجزیه و تست نرم افزار امن می‌باشد. انواع آزمون‌های با ارزش عبارتند از تست نفوذ، تست عملکرد، تست کارایی و تست آسیب پذیری.

دسترس پذیر بودن برنامه‌های کاربردی و داده‌های سازمان که در سرورهای ابر ساکن هستند یک ملاحظه اولیه در به دست آوردن خدمات ابری است. برنامه‌ریزی مداوم کسب و کار و برنامه‌ریزی بازیابی از فجایع فعالیت‌های مهمی برای سازمان هستند رایانش ابری می‌تواند هزینه ورود کمتر در ایجاد قابلیت‌های افزونگی، بهبود، انعطاف‌پذیری پشتیبانی برای سازمان فراهم کند و تداخل بین فرآیندهای کسب و کار را در هنگام و یا پس از یک واقعه مختل کننده کمینه کند.

در بخش پنجم چالش‌های فراروی استفاده از ابر بررسی می‌شود. با پذیرفتن فن‌آوری ابر، چالش‌های بسیاری به خصوص در زمینه محاسبات امن آورده خواهد شد. مدیریت امنیت ابر خصوصی سازمان همینطور نظارت بر اقدامات ارائه‌دهندگان خدمات ابری می‌تواند یک وظیفه به یاد ماندنی تبدیل شود.

برای کمک به کاهش اندازه این وظیفه، ابتکارات مدیریتی که به روشنی تعریف شده‌اند باید برقرار شود تا مالکیت و مسئولیت‌های امنیت داده‌ها را به طور واضح ترسیم کند. بنابراین در این بخش ما تشخیص، جلوگیری و کنترل‌های بهترین شیوه‌های عمل برای تضمین اینکه مجازی سازی باعث شکست وضعیت امنیتی شرکت نشود را بررسی کردیم.

برای رسیدن به این نتیجه ما به لزوم و عملکرد سیاست‌های امنیتی نظر کردیم و بعضی مثال‌ها از اینکه چه نوع سیاست‌هایی معمولاً توسعه می‌یابد ارائه دادیم. ما همچنین از مسئله تشخیص نفوذ کامپیوتری و واکنش به آن و ایجاد تیم‌های واکنش به حوادث امنیتی (CSIRT) یاد نمودیم.

در بقیه بخش بهترین شیوه‌های عمل مدیریت امنیت مجازی سازی‌های مختلف را بررسی کردیم. به بعضی از تهدیدات خاص به محیط مجازی سازی نظر کردیم و سپس بعضی از بهترین شیوه‌های عمل عمومی را امتحان نمودیم و با مشروح تکنیک‌های سخت سازی که منحصر به سیستم‌های مجازی‌سازی بود، بخش را تمام کردیم.

در فصل ششم کتاب به بررسی استانداردهای امنیت ابر پرداختیم [5].

- [1] NIST SP 800-145, The NIST Definition of Cloud Computing.
- [2] NIST SP 500-292, NIST Cloud Computing Reference Architecture.
- [3] ITU-T. X.1601, Cloud computing security – Overview of cloud computing Security.
- [4] Ronald L. Krutz, Russel Dean Vines, " Cloud Security: A Comprehensive Guide to Secure Cloud Computing" Wiley Publishing, Inc ISBN: 978-0-470-58987-8.
- [5] Cloud Security Standards: What to Expect & What to Negotiate, version 2.0, august 2016.

فصل 1 - تعریف رایانش ابری



1-1 - تعریف انستیتوی ملی استانداردها و فن آوری¹ (NIST) از رایانش ابری[1]

رایانش ابری، مدلی است برای امکان پذیر کردن دسترسی به طور فراگیر، آسان، بر اساس تقاضا، از طریق شبکه به استخري از منابع رایانشی قابل پیکربندی (برای مثال شبکه‌ها، سرورها، ذخیره‌سازها، برنامه‌های کاربردی و خدمات) که با حداقل تلاش مدیریتی و یا تعامل با ارائه‌دهنده خدمات می‌توانند به سرعت فراهم و یا رها شوند. این مدل ابری از پنج ویژگی اساسی، سه مدل خدمت و چهار مدل استقرار تشکیل شده است.

1-2 - ویژگی‌های اساسی

1-2-1- خود خدمتی بر اساس بر تقاضا

مصرف کننده می‌تواند به طور یک جانبه توانایی‌های رایانشی خود نظیر زمان استفاده از سرور، ذخیره‌ساز شبکه‌ای را که مورد نیاز است بدون نیاز به تعامل انسانی با هر ارائه‌دهنده سرویس فراهم کند.

1- National Institute of Standards and Technology