



الزامات امنیتی در رایانش ابری

محمد مهدی واعظی نژاد

رایانش ابری، یک فناوری جدید و به عبارتی دیگر، یک نگرش صحیح در طرح‌های سرمایه‌گذاری فناوری اطلاعات است که علاوه بر کاهش شدید هزینه‌ها، عملکرد بهتر و قابلیت‌های فراوانی را به ارمغان آورده است. این فناوری، راهی برای تغییر مدل‌های کسب و کار نبوده، بلکه همچون پدیده اینترنت، انقلابی در زیرساخت‌های فناوری اطلاعات قلمداد می‌شود که معماری نوینی را در توسعه، استقرار، اجرا و ارائه خدمات نرم‌افزاری همراه داشته است.

اکنون شرکت‌های بزرگی همچون مایکروسافت، گوگل و آمازون علاوه بر ارائه نرم‌افزارهای مبتنی بر ابر، اعلام کرده‌اند که اهداف آینده آنها، انتقال برنامه‌های کاربردی به محیط‌های ابری خواهد بود. برنامه‌هایی که روی ابرها مستقر شده و براحتهی همچون ابر روی سرورهای پیشرفته شناورند. پایگاه‌های داده ابری هم توانسته‌اند تحول بزرگی را در تمرکز داده‌ها و اطلاعات ایجاد کنند.

امروزه به‌کارگیری الگوی رایانش ابری – که به‌روزترین و پیشرفته‌ترین فناوری در زمینه زیرساخت‌های فناوری اطلاعات به شمار می‌رود – با بهره‌مندی از قابلیت‌های پویای خود، معمول‌ترین روش برای اشتراک‌گذاری داده‌ها و یکپارچه‌سازی اطلاعات سازمانی است که در کشورهای توسعه یافته جهان، زیرساخت‌های آن بسرعت در حال توسعه و خدمات مبتنی بر ابر نیز رو به گسترش است.

در رایانش ابری، سازمان‌ها می‌توانند ضمن کاهش شدید هزینه‌ها، از طریق ادغام سیستم‌ها و تجهیزات سخت‌افزاری و به اشتراک‌گذاری آنها براساس نیاز کاربران، محیطی پویا در ارائه خدمات ایجاد کرده که علاوه بر مالکیت سیستم، هزینه‌های تعمیر و نگهداری آن، تهیه نسخه‌های پشتیبان از اطلاعات و استخدام کارشناسان فنی، به ارائه‌کنندگان خدمات ابری واگذار می‌شود.

مدل‌ها و الگوهای رایانش ابری

مدل‌های سرویس ابری و الگوهای استقرار ابرها را می‌توان به موارد مختلفی تقسیم‌بندی کرد.

براساس مدل‌های سرویس ابری، ارائه‌کنندگان خدمات ابری به سه دسته تقسیم می‌شوند:

برنامه‌های کاربردی در ابر (نرم‌افزار به عنوان یک سرویس - SaaS): در این مدل، برنامه‌های کاربردی از طریق یک رابط کاربری سبک مانند مرورگر وب، روی زیرساخت‌های ابری اجرا می‌شود.

در این نوع مدل از خدمات ابری، امنیت و حفاظت از حریم خصوصی به عنوان بخشی جدایی‌ناپذیر از SaaS، به دریافت‌کنندگان خدمات ارائه می‌شود.

سیستم عامل در ابر (پلتفرم به عنوان یک سرویس - PaaS): این مدل، توانایی استقرار یا به دست آوردن برنامه‌های نوشته شده با استفاده از زبان‌های برنامه‌نویسی و ابزارهای پشتیبانی آن را از سوی ارائه‌کننده خدمات ابری، در اختیار دریافت‌کنندگان قرار می‌دهد.

در این نوع مدل، برنامه‌های کاربردی مورد استفاده، قابل پیکربندی و کنترل بوده و تلاش می‌شود با ساز و کارهای امنیتی اساسی در ارائه‌کننده خدمات ابری مانند رمزگذاری اطلاعات، تأیید هویت و مجوزهای لازم و همچنین در سطح برنامه‌های کاربردی، با تعیین میزان دسترسی و کنترل آن، سازوکارهای حفاظتی لازم برای تأمین امنیت و حفظ حریم خصوصی ایجاد شود.

زیرساخت در ابر (زیرساخت به عنوان یک سرویس - IaaS): در این مدل، ارائه پردازش، ذخیره‌سازی، کنترل محدود امور شبکه‌ای (مانند فایروال‌ها)، بعضی از منابع محاسباتی، اجرا و کنترل نرم‌افزارهای دلخواه شامل سیستم عامل و برنامه‌های کاربردی، توسط دریافت‌کنندگان خدمات ابری، قابل تنظیم است.

در این مدل از خدمات ابری، توسعه‌دهندگان نرم‌افزارها، مسئول کامل حفاظت از امنیت و حفظ حریم خصوصی دریافت‌کنندگان خدمات، به شمار می‌روند.

مدل‌های استقرار رایانش ابری نیز به موارد زیر تقسیم می‌شود:

ابر خصوصی: زیرساختی ابری بوده که فقط برای یک سازمان اجرا شده و متعلق به آن است.

لحاظ کردن نکات امنیتی و حفاظت از حریم خصوصی کسانی که در یک مجموعه ابر خصوصی هستند، به‌عنده ارائه‌کننده آن خدمات ابری است.

ارتباطات ابری: زیرساخت ابری به اشتراک گذاشته شده از سوی چند سازمان که نیازمندی‌ها و نگرانی‌های مشترکی مانند مأموریت‌ها، سیاست‌ها، کنترل‌های امنیتی و سایر ملاحظات را دارند.

ابر عمومی: زیرساخت ابری که در دسترس عموم مردم یا یک گروه صنعتی بزرگ بوده و متعلق به یک ارائه‌کننده خدمات ابری است.

در این نوع مدل از استقرار ابری، توسعه‌دهندگان نرم‌افزار و ارائه‌کنندگان خدمات ابری، مسئول حفاظت از امنیت و حفظ حریم خصوصی کاربران خود هستند. به طور خلاصه، باید اذعان کرد که امنیت و حفظ حریم خصوصی، بسیار فراتر از اجرای دسترسی‌های کاربری و رمزهای عبور بوده و به‌کارگیری و اعمال الزامات امنیتی ضرورتی بزرگ برای سیستم‌هایی است که از اطلاعات حساس و حیاتی برخوردار هستند.

از آنجا که امنیت و حفظ حریم خصوصی و همچنین حفاظت از اطلاعات، از بالاترین درجه اهمیت برخوردار است، می‌توان سه اصل مهم را برای اطمینان از حفظ حریم خصوصی، صحت محتوا و قابلیت اعتماد منابع اطلاعاتی در نظر گرفت. اول این که تمامی اطلاعات باید از طریق رمزنگاری توسط مالکان آنها کنترل، محافظت، ذخیره‌سازی، انتقال و در دسترس امن قرار گیرند. دوم این که در ایجاد و نگهداری اطلاعات باید اصالت محتوا و جامعیت داده‌ها با توجه به امکان سفارشی کردن حفظ حریم خصوصی کاربران در فرآیندهای ادغام اطلاعات و داده‌ها در نظر گرفته شود و سوم، دسترسی و به اشتراک‌گذاری اطلاعات باید از طریق امضای دیجیتال و فرآیندهای صدور گواهینامه به منظور جلوگیری از تغییرات غیرمجاز در محتوای اطلاعات حساس، صورت گیرد.

گرچه بعضی از نیازهای امنیتی و حفظ حریم خصوصی در برنامه‌های ابری به مدل سرویس یا استقرار ابری مورد استفاده بستگی دارد، اما با اجرای دقیق یک مدل مبتنی بر ابر، می‌توان بالاترین سطوح امنیت فیزیکی، شبکه‌ای، برنامه‌های کاربردی، داده‌ها و سیستم‌های داخلی را تضمین کرد که استراتژی‌هایی همچون تهیه نسخه‌های پشتیبان از اطلاعات، روش‌ها و سیاست‌های امن داخلی، شیوه‌های استاندارد تنظیمات امنیتی و صدور گواهینامه‌ها نیز در بطن آن گنجانده شده است. موارد مهمی همچون رمزنگاری اطلاعات و احراز هویت کاربران نیز به طور مرتب در حال اجراست.

پانویس‌ها:

- 1 - Software as a Service
- 2 - Platform as a Service
- 3 - Infrastructure as a Service

