1st International Conference
on new achievements in
Science & Technology
24th August 2017

اولین کنفرانس بین المللی
دستاوردهای نوین در
علوم و تکنولوژی
۲ شهریور ماه ۱۳۹۶ – تهران

معماری مبتنی بر مدل پیشگیرانه برای امنیت در محاسبات ابری

مجید پیوسته[۱]

۱- دانشجوی کارشناسی ارشد مهندسی کامپیوتر نرم افزار-دانشگاه آزاد اسلامی واحد کرمانشاه

چکیده

سازمان ها به طور فزاینده ای نسبت به محاسبات ابر به عنوان یک تکنولوژی جدید انقلابی متعهد هستند که قصد کاهش هزینه های IT و دستیابی به چابکی در عملیات را داشته باشند. این تلاش با چالش های قابل توجهی از امنیت مواجه شده است، که موجب معضل این است که آیا این فناوری جدید امیدوارکننده را می پذیرد یا خیر. این مسئله با این واقعیت که مشتری باید به ادعاهای قابلیت های امنیتی ارائه دهنده سرویس ابر، با نظارت و اعتبار سنجی کم یا بدون آن تکیه کند، تشدید می شود. در این مقاله، ما چشم انداز امنیتی را به طور جزئی تجزیه و تحلیل می کنیم و معماری را بر اساس یک مدل پیشگیرانه ارائه می دهیم که به طور جامع به این مسئله فزاینده دشوار می پردازد. یک ابر امنیتی به طور جدی ارائه دهنده خدمات ابر را برای نقض قوانین نظارت می کند. هر گونه نقض سیاست گزارش شده و بر این اساس، مشتری تصمیمات امنیتی را مطلع می کند.

کلمات کلیدی :محاسبات ابری، امنیت، سیاست ابری، ابر امنیتی

معرفی

سازمانها در سراسر جهان مزایای زیادی از فناوری اطلاعات را به عنوان یک راننده جدید برای تغییر و نوآوری به دست آورده اند. اما تلاش انسان برای نوآوری هرگز به پایان نمی رسد و فناوری جدید امیدوار کننده در عصر Cloud Computing است.

بر طبق NIST، محاسبات ابری به عنوان یک مدل برای دسترسی به شبکه دسترسی آسان و مناسب به یک استخر مشترک از منابع محاسباتی قابل تنظیم (مانند شبکه ها، سرورها، ذخیره سازی، برنامه ها و سرویس ها) تعریف می شود که می تواند به سرعت در اختیار و منتشر شود

تکنولوژی ابر روند رو به رشد است.

سازمان ها در سراسر جهان نشسته و متوجه این پدیده جدید هستند که وعده های هنگفت هزینه ها، چابکی و مقیاس پذیری را به شرکت های بزرگ یا کوچک می دهد.

محققان در سالهای آتی پیش بینی رشد چشمگیری داشته اند.

با وجود وعده ها، پارادایم Cloud Computing یک مشکل چشمگیر دارد: امنیت.

از آنجا که ابر یک پارادایم جدید است، برنامه ریزی دقیق و اعدام را شامل می شود. این امر باعث می شود که سازمان فقط برای پریدن در راه پیمایشی بدون برنامه ریزی و استراتژی مناسب جایگزین شود.

این نگرانی در واقع در نظرسنجی هایی است که امنیت را به عنوان بزرگترین نگرانی برجسته می کند.

زمینه

با توجه به NIST، مدل ابر از چهار ویژگی اساسی تشکیل شده است.

چهار ویژگی اساسی به شرح زیر است:

خودپرداز بر روی تقاضا

دسترسی به شبکه گسترده

جمع آوری منابع

کشش سریع

خدمات اندازه گیری مدل خدمات به شرح زیر است:

نرم افزار به عنوان یک سرویس :SaaS

از سرویس دهنده استفاده می کند

برای مثال برنامه های کاربردی بیش از یک شبکه، Google Docs.

ذخیره سازی، ظرفیت شبکه و دیگر منابع محاسباتی اساسی برای مثال .Salesforce.com

مدل های استقراری که می توانند به صورت داخلی یا خارجی اجرا شوند، در ارائه NIST به شرح زیر خلاصه می شوند:؟ ابر خصوصی - سازمانی متعلق به یا اجاره شده است؟ ابر جامعه - زیرساخت مشترک برای منافع مشترک مشترک خاص؟ ابر عمومی - به عموم، زیربنای مقیاس بزرگ به فروش می رسد؟ ابر ترکیبی - ترکیب دو یا بیشتر ابرها یکی دیگر از ویژگی های در نظر گرفته شده است چند اجاره.

اگرچه مستقیما پوشش داده نمی شود، مستغلات چندگانه به عنوان یکی از ویژگی های اساسی پارادایم در نظر گرفته می شود و اجازه می دهد تا هزینه های به اشتراک گذاری و اقتصاد مقیاس.

لازم به ذکر است که مزایای ابر ذکر شده در بالا بیشتر زمانی که یک مدل Cloud Cloud انتخاب می شود، افزایش می یابد.
ارائه دهندگان خدمات ابری (CSP ها) اقتصاد مقیاس را به دلیل استفاده از زیرساخت های زیربنایی توسط بسیاری از مشتریان اهرمی می کنند.
استفاده مجدد از زیرساخت ها موجب می شود تا مزایای کاهش هزینه ها به مشتریان منتقل شود.

تجزیه و تحلیل امنیت ابر

به منظور تجزیه و تحلیل، ما دو مدل اولیه گسترش ابر، خصوصی و عمومی را در نظر می گیریم و مناسب بودن آنها را برای پذیرش در محیط سازمانی بررسی می کنیم.
ابرهای جامعه و ابر ترکیبی مشتق از دو فوق هستند. از این رو، ما نگرانی خود را نسبت به مدل ابر خصوصی و عمومی ابراز می کنیم.
پارادایم محاسبات ابری راه های جدیدی از حمله را باز می کند و از این رو چندین مسائل امنیتی در صورت پذیرش آن ایجاد می شود.
مسائل مربوط به امنیت ابر بالا با توجه به Cloud Security Alliance عبارتند از:

سوء استفاده و استفاده نادرست از ابر رایانه

ارائه دهندگان سرویس Cloud به طور معمول راه حل های IaaS و PaaS را برای چندین مشتری ارائه می دهند.
این کار آنها را قادر می سازد هزینه های زیرساخت را در بسیاری از سازمان ها توزیع کنند.
این به شدت اقتصاد پدیده مقیاس است. هرچه تعداد مشتریان بیشتر باشد، برای ارائه دهنده ارزان تر است. برای بهبود چشم انداز کسب و کار، اغلب آزمایشی رایگان به مشتری آینده نگر ارائه شده، در بسیاری موارد با یک الزام فقط یک کارت اعتباری معتبر.
این به جنایتکاران اینترنتی کمک می کند و از زیرساخت های CSPs آسیب پذیر برای اهداف نابکار مانند اسپم، فیشینگ و بوت نت استفاده می کند.
این ممکن است در کل محدوده IP آدرس ارائه دهنده خدمات، پایان دادن به یک لیست سیاه.
بنابراین، یک ابر عمومی با چنین مسائلی روبرو است، که اغلب از سوی منافع ارائه دهنده خدمات به مزایای این پیشنهادات محرمانه تشدید می شود.

Interfaces Unsafe and APIs

CSP ها API های مختلفی را برای تهیه، مدیریت، ارکستراسیون و نظارت برابر به مشتریان ارائه می دهند.
امنیت ابر بستگی به مجموعه ای از API ها که به صورت عمیق انجام می شوند و مسئولیت عملکرد از طریق احراز هویت برای دسترسی به کنترل است.
هر گونه اشکال می تواند ویرانی و امنیت کامل ابر را به خطر بیندازد. جنایتکاران سایبری ممکن است حتی قادر به ورود به سیستم ناشناس باشند. نیازی به گفتن نیست، این یک چشم انداز تهدید کننده برای موقعیت امنیتی یک سازمان است.

هر دو ابرهای عمومی و خصوصی تحت این تهدید هستند.
بهترین پیشگیری در برابر تهدید داخلی، یک سیاست امنیتی قوی و موثر سازمان است.
هرگونه عدم تطابق باید شدید مجازات شود. دعوی قضایی بازدارنده موثر در این مورد است. امنیت سازمان با استفاده از سرویس های ابری اغلب توسط نوع افرادی که توسط ارائهدهنده خدمات Cloud استخدام می شوند، مستقل است.
مشتریان هیچ خط مستقیم در سیاست های استخدام چنین ارائه دهندگان ندارند. حوادث جاسوسی شرکتی که در آن یک رقیب عمدا یک مول را ایمپلنت می کند
در شبکه ارائه دهنده نمی تواند به طور کامل رد شود.
متاسفانه Cloud Clouds به طور جدی تحت تاثیر این نقص قرار دارند.

مسائل مربوط به فناوری اشتراکی

فروشندگان IaaS معماری متعدد مستاجر را به منظور دستیابی به مقیاس اقتصادی در عملیات خود می پذیرند.
مجازی سازی و به ویژه محصولات مبتنی بر Hypervisor برای این منظور استفاده می شود.
این نتیجه در سناریویی است که زیرساخت توسط بسیاری از مشتریان مختلف به اشتراک گذاشته شده است.
الزامات امنیتی اغلب وابسته به قابلیت اعتماد hypervisor است.
تحقیقات نشان داده است که مهاجم مخرب ممکن است اعتبار سنجی و امنیت hypervisor را به منظور دستکاری سایر ماشین های مجازی مهمان در حال اجرا و تاثیر حمله DoS متوقف کند.
علاوه بر این، می توان یک توافق جامع را رد کرد که می تواند امنیت داده های مربوط به مشتری را تحت تأثیر قرار دهد.
باز هم، ابرهای عمومی به طور مستقیم تحت تاثیر این تهدید قرار می گیرند. از سوی دیگر، ابرهای خصوصی نیز ممکن است آسیب پذیر باشند. به طور معمول، یک ابر خصوصی، تنها ماشینهای مجازی متعلق به یک دامنه امنیتی یک سازمان را اجرا می کند.

Cloud Cloud: Affected Cloud Private: Affected Loss of Data or Leakage

از بین رفتن داده یا نشت غیر مجاز به شخص ثالث یکی از بزرگترین تهدیدات در عرصه رایانه است.
با توجه به اینکه مدل Cloud Computing ساختار یافته است، داده های سازمان ممکن است در سرورهای دیگری در یک کشور به پایان برسد.
این نگرانی مهم برای برخی از سازمان ها است. مسئله دیگر این است که چه مدت ممکن است داده ها توسط سرویس دهنده خدمات Cloud حفظ شود.
داده ها ممکن است همچنان در سرورهای ارائه دهنده باقی بمانند حتی پس از حذف توسط مشتری.
همچنین، ارائه دهنده ممکن است به طور غیرمستقیم، کپی های اضافی داده ها را به منظور فروش آن به اشخاص ثالث مورد علاقه، حفظ کند.
مطمئنا، رمزگذاری می تواند به عنوان یک راه حل مورد استفاده قرار گیرد اما تمام مسائل را حل نمی کند.
حفظ حریم خصوصی و انطباق با مقررات ممکن است نیاز به داده نداشته باشد که از صلاحیت یک کشور عبور کند.
علاوه بر این، چشم انداز اطلاعاتی که توسط دولت خارجی مصادره می شود، قابل رد نیست.

وضعیت ژئوپلیتیک حاکم بر ایمنی داده ها نیز بسیار کم است.
ابرهای عمومی قطعا تحت تاثیر همه تهدیدهای فوق قرار دارند.

حساب یا سرویس ربودن

به طور معمول یک ابر با استفاده از احراز هویت در قالب کلمه عبور به یک ابر دسترسی پیدا می کند.
در ابر عمومی، تهدید حساب کاربری هک شده بسیار بالا است. حتی تأیید صحت دو فاکتور ممکن است در مورد یک ویروس مخرب در توافق نهایی سرویس گیرنده با مهاجمان موثر باشد.
این ممکن است منجر به وضعیتی شود که مهاجمان ممکن است قادر به دسترسی به کل اطلاعات حساس باشند.
باز هم ابرهای عمومی از این تهدید به طور مستقیم تحت تاثیر قرار می گیرند.
پروتکل ها باید به منظور ارائه سطح قابل قبول امنیت مورد استفاده قرار گیرد.
سیاست ابر به منظور رفع چنین مشکلی و تلاش برای طراحی دقیق نیازهای امنیتی یک سازمان به عنوان رایانش ابری را تصویب می کند.
داشتن یک سیاست ابر منحصر به فرد، مزایای مشخص کردن همه مسائل امنیتی Cloud را در یک مکان که توسط کل سیاست امنیتی سازمان تحت تاثیر قرار می گیرد، فراهم می کند.

متدولوژی پیشگیرانه

همانطور که قبلا ذکر شد، بسیاری از تهدیدات به علت اختلاف در علاقه به هدف کسب و کار ارائه دهنده در مقابل نیاز امنیتی توسط سازمان، بوجود می آیند.
یک مثال میتواند انتخاب کننده ارائه دهد که اجازه انجام دادن ارائه محاکمه آزاد را نخواهد داد که درب را برای تخلفات غیرقانونی و سوءاستفاده از مجرمان سایبری باز کند.
ثانیا، باید اطمینان حاصل شود که ارائه دهنده خدمات دارای یک سیاست استخدام مناسب است که به خوبی منطبق با سیاست منابع انسانی (سازمان منابع انسانی) سازمان است.
این تضمین می کند که کارمندان ناراضی ارائه دهنده به طور غیر مستقیم بر سازمان تاثیر نمی گذارد.
در نهایت باید یک SLA بسیار مشخص (توافق نامه سطح خدمات) مورد نیاز باشد که به وضوح میزان امنیت مورد نیاز شامل ارزیابی تهدیدات دوره ای شبکه ارائه دهنده و اطلاعات در صورت وقوع یک رویداد امنیتی را مشخص می کند.
تعهد به مراقبتی قابل توجه توسط ارائه دهنده باید مورد توجه قرار گیرد. ارائه دهنده خدمات این را با اجرای بهترین شیوه های امنیتی برای نصب و پیکربندی و ارسال یک گزارش دوره ای به مشتری نشان می دهد.

دسترسی مجاز کاربر: ارائه دهنده باید پاسخگو باشد برای افرادی که برای مدیریت داده های سازمان استخدام شده اند.
فقط ارائه دهندگان با یک سیاست سازگار با منابع انسانی باید قرارداده شوند.
رعایت مقررات: ارائه دهنده باید مایل باشد که به ممیزی های شخص ثالث بپردازد و به دغدغه های قانونی توجه کند.

در مورد PCI DSS، بایگانی داده ها باید به تنظیم کننده ها و مدیران امنیتی ارائه شود.

موقعیت داده: داده ها در یک زیرساخت ابر عمومی ممکن است به دور و گسترده سفر کنند. استقلال محل در واقع یکی از اصول محاسبات ابری است. ارائه دهنده باید نگرانی ها را از بین ببرد، اگر هر یک از سازمان ها در مورد مکان داده.

در صورت نیاز، ارائه دهنده باید تمایل خود را برای محدود کردن جریان داده ها از مرزهای کشور مورد نظر نشان دهد.

تقسیم اطلاعات: کارشناسان باید طرح های رمزنگاری را در استفاده ارزیابی کنند و آنها را به عنوان ایمن تایید کنند. ارائه دهنده ابر باید فقط از الگوریتم های رمزنگاری استاندارد و پروتکل ها استفاده کند.

بازیابی: در صورت وقوع یک فاجعه، داده ها باید از چندین سایت قابل بازیابی باشند، در صورت نیاز.

این به ارائه دهنده خدمات نیاز دارد تا یک سیاست جامع تداوم کسب و کار و برنامه ریزی برای بازیابی فاجعه در نظر بگیرد.

همچنین زمان لازم برای بهبودی از یک حادثه باید پس از آن و تضمین ایجاد شود.

پشتیبانی تحقیقاتی: بررسی فعالیت غیرقانونی در یک محیط ابر به ویژه دشوار است.

گارتنر پیشنهاد می کند که ممکن است پشتیبانی از طرف ارائه کننده برای این امر غیرممکن باشد.

حیثیت بلند مدت: خرید و ادغام در پایان سرویس دهنده می تواند مشکل تدارکاتی ایجاد کند

معماری بر اساس روش پیشگیرانه

دسترسی به داده ها مجوز مشخصی از آنچه در واقع به داده ها در چنین وضعیتی اتفاق می افتد، باید دنبال شود.

علاوه بر این، موارد زیر باید در نظر گرفته شود:؟ فن آوری های غیر اختصاصی: این برای جلوگیری از قفل کردن فروشنده است.

برخی ابرها با دیگران ناسازگار هستند. به عنوان مثال، مایکروسافت ابرها با آنهایی که گوگل ناسازگار هستند. با توجه به انعطاف پذیری بیشتر، باید یک ارائه دهنده ای که از OVF (Open Virtualization Format) پشتیبانی می کند، انتخاب شود.

مدیریت داده ها: این باید سیاست های دقیق مدیریت داده که توسط ارائه دهنده خدمات پذیرفته شده است، توصیف شود.

جزئیات کامل مربوط به اینکه چه کسی دسترسی به داده ها دارد، چه اقداماتی می تواند انجام شود، باید به صورت شفاف بیان شود.

امنیت برنامه: باید تست های امنیتی دوره ای انجام شود. ویژگی های امنیتی و الزامات تعریف شده باید توسط ارائه دهنده پیگیری شود.

الزامات امنیتی برای برنامه باید توسط تیم امنیتی به توسعه دهندگان ارائه شود.

مدل امنیتی رابط های ارائه دهندگان ابر: همانطور که در بالا توضیح داده شد، API های ناامن تهدید جدی امنیتی می کنند.

از این رو، مدل امنیتی اینترفیس ها باید به طور دقیق ارزیابی شود. ؟ سیاست ارائه دهندگان منابع انسانی: همانطور که قبلا بحث شد، بسیار ضروری است که سیاست های منابع انسانی ارائه دهنده مورد بررسی قرار گیرد.

حذف امن داده ها: در ابرهای عمومی، به دلیل چند اجاره، ممکن است مهاجم یک استخر بزرگ فضای دیسک را بدست آورد و آن را برای بقایای داده تجزیه و تحلیل کند

نظارت بر فهرست های سیاه و سفید عمومی برای بلوک های شبکه شخصی خود: همانطور که در تهدیدات برتر امنیتی ابر بحث می شود، این مرحله برای اطمینان از اینکه بلوک شبکه ای که توسط CSP استفاده می شود به دلیل فعالیت غیرمجاز هرزنامه، انکار وضعیت سرویس برای مشتری.

ارزیابی آسیب پذیری: با استفاده از ابزارهای خودکار، اسکن آسیب پذیری منابع شبکه CSP تضمین می کند که سلامت فعلی شبکه ارائه دهندگان می تواند اندازه گیری شود.

تست نفوذ: ابزار تست نفوذ اتوماتیک مانند چارچوب Metasploit می تواند برای آزمایش شبکه CSP استفاده شود.

باید مراقب باشیم که باعث ایجاد اختلال در خدمات در شبکه ارائه دهنده خدمات نشود که هدف کل تمرینات را برطرف می کند.

برای حصول اطمینان از آزمون جامع، چارچوب تست نفوذ از منبع باز مانند OSSTMM می تواند مورد استفاده قرار گیرد.

ورود به سیستم تجزیه و تحلیل: افشای سیاههها قابل اجرا و داده های مربوط به CSP توسط سیاست ابر اختصاص داده شده است.

این تجزیه و تحلیل ورودی توسط ابر امنیتی انجام می شود که هرگونه نقض مدیریت را گزارش می دهد.

سیستم پیشگیری از نفوذ میزبان: در مدل IaaS، CSP تنها برای منابع اساسی مانند ذخیره سازی و شبکه سازی فراهم می کند.

انتظار می رود که سرویس گیرنده برای سیستم عامل ها و برنامه های کاربردی ارائه کند. با استفاده از HIPS)سیستم پیشگیری از نفوذ بر اساس میزبان) می تواند به عنوان یک روش دفاع در عمق اعمال شود.

با استفاده از تشخیص آنومالی و تجزیه و تحلیل پروتکل حسی، یک سیستم موثر می تواند طراحی شود.

مزایای آرشیو پیشنهاد شده بر اساس مدل پیشگیرانه

دو رویکرد مرحله ای، مدیران شبکه و توسعه دهندگان را با درکی کلیدی در پارادایم ابر می سازد، بنابراین از شوک فرهنگی که ممکن است در صورت پذیرش عمومی Cloud در یک زمان اتفاق بیفتد، اجتناب از شوک فرهنگی ایجاد شود، در نتیجه سازمان را به تهدیدات ناشناخته منتقل می کند.

خدمات اضافی ارائه شده مانند ترویج آسیب پذیری و تست نفوذ امنیت کلی را بهبود می بخشد.

ارائه دهنده خدمات Cloud به دقت مورد بررسی قرار میگیرد و به دقت مراقبتی است که به شدت تحت نظارت است که وضعیت امنیتی کلی مشتری را بهبود میبخشد.

در نهایت، بهبود مداوم سیاست ابر به موجب پیشرفت های جاری در فن آوری های امنیتی ابر، اطمینان حاصل می کند که این معماری در تامین نیازهای جدیدترین تهدیدات امنیتی باقی می ماند.

نتیجه

ابر رایانه به عنوان یک فن آوری هنوز در حال تکامل است.

این صنعت در حالی که کارشناسان این معایب را از بین می برد، با نفس نفس می کشد. با توجه به مسائلی که شایع هستند، یک روش پیشگیرانه برای پذیرش Cloud Computing توصیه می شود.

نظارت مداوم برای هر گونه نقض قوانین به خوبی برای سازمان ها بسیار مفید است، زیرا اکنون کنترل بیشتری بر امنیت ابر عمومی دارند و نه فقط به اطمینان از طرف فروشندگان تکیه می کنند.

ما اطمینان داریم که این رویکرد وضعیت امنیتی ابرهای عمومی را بهبود می بخشد و راه های زیادی برای سرعت بخشیدن به پذیرش سازمان های سراسر جهان خواهد داشت.

منابع

[1] National Institute of Standards & Technology (NIST), http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc, November 2010
[2] Gartner Newsroom, http://www.gartner.com/it/page.jsp?id=1389313, January 2011
[3] The Data Center Users' Group DCUG Spring survey 2010, http://www.datacenterug.org/profiles/blogs/data-center-users-groupsurvey, January 2011
[4] Windows Azure, http://www.microsoft.com/azure/whatisazure.mspx, November 2010
[5] Google Docs, http://docs.google.com/, November 2010
[6] Salesforce.com, http://www.force.com/, November 2010
[7] Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, Inc. 2010
[8] Cloud Security Alliance, Top Threats to Cloud Computing V1.0, http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, December 2010
[9] CERT Insider Threat Research, 2010 CyberSecurity Watch Survey, http://www.cert.org/archive/pdf/ecrimesummary10.pdf/, December 2010
[10] Novell survey, http://www.informationweek.in/Cloud_Computing/10-10-05/Novell_survey_reveals_widespread_enterprise_adoption_of_private_clouds.aspx , January 2011
[11] Kresimir Popovic and Zeljko Hocenski , "Cloud computing security issues and challenges," in Proceedings of the 33rd International Convention, MIPRO 2010
[12] Gartner Seven Security Risks of Cloud Computing, http://www.networkworld.com/news/2008/070208-cloud.html, January 2011
[13] NIST Special Publication 800-88: Guidelines for Media Sanitization http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf, February 2011
[14] Metasploit Framework, http://www.metasploit.com/framework/, December 2010
[15] Open Source Security Testing Methodology Manual, www.isecom.org/osstmm/, January 2011
[16] The NIST Guide to Intrusion Detection and Prevention Systems (IDPS) http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, January 2011
[17] John the Ripper Password Cracker, http://www.openwall.com/john/, January 2011
[18] THC-Hydra Network Logon Cracker, http://thc.org/thc-hydra/, January