



خبرنامه

فاوای نفت



تاریخ انتشار ۹۵/۰۴/۰۲ شماره خبرنامه ۲۵۶

ماموریت مدیریت فاوای نفت، تحول به صنعت نفتی - یادگیر بیشتر و صاحب اندیشه و خرد

دستیابی به صنعت نفتی مبتنی بر اندیشه و خرد با محوریت فاوا
ارتقای دانش با محوریت سرمایه فکری به منظور افزایش کارایی و اثربخشی
ایجاد بسترهای مناسب و مطلوب فاوا جهت دستیابی به صنعت نفت پیشرفته
ارتقاء کارایی و اثربخشی ارکان مدیریتی و اجرایی از طریق فاوا در صنعت نفت
برنامه‌ریزی و هوشمند سازی فرایندهای کسب و کار الکترونیک صنعت نفت
استقرار فراگیر و یکپارچه کاربردها و خدمات فاوا در صنعت نفت



صنعت ۴.۰



وب ۲.۰



امنیت



آموزش

در این شماره می‌خوانید:

- خدمات ابری میکروسافت
- دسترسی به اینترنت
- حفره امنیتی
- درآمد SAP
- اوراکل

خبرنامه فاوای نفت از علاقه‌مندان در خصوص
ارائه مطلب و پیشنهادات دعوت به مشارکت می‌نماید



مایکروسافت در کنفرانس بین‌المللی خود موسوم به Worldwide Partner Conference که هر ساله با حضور شرکایش برگزار می‌کند، از برنامه‌ها و خدمات جدیدش برای ویندوز ۱۰ رونمایی کرد. در این کنفرانس که چندی پیش در تورنتو برگزار شد، سرویس اشتراکی جدید ویندوز یعنی «اشتراک سرویس ابری برای کسب و کارهای کوچک» معرفی شد. به گزارش بلومبرگ، از پاییز امسال نسخه Enterprise ویندوز ۱۰ که مجهز به قابلیت‌های امنیتی بیشتر است، به بهای ۷ دلار در ماه به ازای هر کاربر، در اختیار مشتریان برنامه Cloud Solution Provider مایکروسافت قرار خواهد گرفت.

پیش از این، برنامه مزبور عمدتاً به شرکت‌های بزرگتر تعلق می‌گرفت ولی اکنون اندازه شرکت مطرح نیست و حتی کسب و کارهای کوچک نیز می‌توانند از این نسخه ویندوز بهره‌مند شوند. مت بارلو (Matt Barlow) مدیر بازاریابی ویندوز مایکروسافت می‌گوید این، قیمت یک فنجان قهوه و یک دونات است!

بر اساس این گزارش، مایکروسافت برای رواج برنامه‌های خود از جمله ویندوز ۱۰ یک ساله، چشم امید به ابر و کسب و کارهای کوچک دارد. این نخستین بار است که شرکت‌ها می‌توانند با استفاده از فضای ابری، Windows Enterprise Edition را به‌روز و مدیریت کنند.

۵۳ درصد مردم جهان هنوز به اینترنت دسترسی ندارند

در حالی که هم‌اکنون نیمی از کاربران جهانی بازی Pokemon را روی دستگاه موبایلی خود نصب کرده‌اند، نیم دیگر ساکنان کره خاکی هنوز به اینترنت دسترسی ندارند. به گزارش وبسایت pcworld، حدود ۳.۹ میلیارد نفر معادل ۵۳ درصد ساکنان کره زمین تا پایان سال ۲۰۱۶ میلادی آنلاین خواهند بود و این آماری است که اتحادیه جهانی مخابرات (ITU) در جدیدترین گزارش خود به آن اشاره کرد. حتی در اروپا که متصل‌ترین منطقه جهان محسوب می‌شود، ۲۰.۹ درصد مردم هنوز آنلاین نشده‌اند. در آفریقا که کمترین میزان اتصال مردم به اینترنت گزارش شده است ۷۴.۹ درصد از مردم هنوز آنلاین هستند.

این آمار و ارقام بخشی از پیش‌بینی‌های سالانه آژانس ITU وابسته به سازمان ملل متحد محسوب می‌شود. در این گزارش همچنین نشان داده شد بین کشورهای فقیر و غنی شکاف بزرگی وجود دارد و از نظر جنسیتی، میزان دسترسی کاربران زن و مرد به اینترنت هم بسیار متفاوت است. به نظر می‌رسد طرح‌های شرکت‌های بزرگی چون گوگل و فیسبوک برای دسترسی همه مردم جهان به اینترنت به زمان زیادی نیاز داشته باشد.

با توجه به اینکه چهار نفر از هر پنج فردی که ساکن کشورهای توسعه یافته هستند به اینترنت دسترسی دارند، این رقم برای کشورهای در حال توسعه ۴۰ درصد گزارش شده است. در گزارش «کشورها با کمترین میزان توسعه‌یافتگی» سازمان ITU شامل هائیتی، یمن، میانمار و اتیوپی تنها ۱۵.۲ درصد مردم آنلاین هستند.

همچنین گفته شده است درصد زنان آنلاین نسبت به مردان کمتر است. تفاوت ضریب نفوذ اینترنت بین زنان و مردان ۱۲.۲ درصد گزارش شده است که این رقم برای سال ۲۰۱۳ میلادی تنها ۱۱.۰ درصد بود. سازمان ITU همچنین اعلام کرد این رقم در کشورهای توسعه یافته از ۵.۸ درصد به ۲.۸ درصد کاهش یافته و در عوض در کشورهای فقیر رو به افزایش است.

کشف حفره امنیتی بسیار خطرناک در مرورگر Silk آمازون



مرورگر اینترنتی Silk آمازون یک حفره امنیتی بسیار جدی را شامل می‌شود که نه تنها استانداردهای امنیتی SSL را در جست‌وجوهای گوگل نادیده می‌گیرد، بلکه از انتقال فعالیت‌ها به نسخه ایمن موتور جست‌وجو جلوگیری می‌کند.

به گزارش وبسایت Zdnet، مرورگر اینترنتی Silk که مبتنی بر Chrome گوگل ساخته شده است، روی تبلت‌های Kindle آمازون در اختیار کاربران قرار می‌گیرد و بدون فناوری امنیتی Secure Sockets Layer یا SSL فعالیت می‌کند. این فناوری ارتباطات میان سرورها و مرورگرهای اینترنتی را رمزگذاری می‌کند و همچنین از تاییدیه‌های خودکار به نسخه SSL گوگل برای موتور جست‌وجوی این شرکت اینترنتی جلوگیری می‌کند.

این مشکل امنیتی باعث می‌شود ارتباطات کاربران بدون اینکه رمزگذاری شوند ناایمن باقی بمانند و امکان ورود حملات میان‌افزارها فراهم شود. مرکز امنیتی Nightwatch Security با کشف این حفره امنیتی، اطلاعات مربوط به آن را به صورت عمومی منتشر کرد. این گروه امنیتی توضیح داد که مرورگر اینترنتی آمازون که به کاربران امکان می‌دهد بین جست‌وجوهای اینترنتی گوگل، بینگ و یاهو یکی را انتخاب کنند، در صورت انتخاب جست‌وجوگر گوگل از فناوری SSL استفاده نمی‌کند. گروه امنیتی مذکور توضیح داد: «تمامی جست‌وجوهای انجام شده از طریق این مرورگر اینترنتی بدون در نظر گرفتن استاندارد HTTPS انجام می‌شود و این مسئله باعث می‌شود کدهای مخرب بتوانند ترافیک مخصوص موتور جست‌وجوی انتخاب شده از سوی کاربر را مانیتور کنند».

آمازون با خرید Cloud۹ به دنبال تقویت AWS است



شرکت آمازون با هدف افزودن برخی قابلیت‌های جدید به سرویس ابری خود (AWS)، استارت‌آپ Cloud۹ را خریداری کرد. به گزارش وبسایت ITProPortal، شرکت آمریکایی Cloud۹ در سال ۲۰۱۰ راه‌اندازی شده و به توسعه‌گران این امکان را می‌دهد که از راه دور با یکدیگر همکاری داشته باشند و کدها را توسعه دهند و یا ویرایش و تست کنند.

Cloud۹ از ۳۰۰ مبرورگر و سیستم عامل مختلف و از ۴۰ زبان برنامه‌نویسی پشتیبانی می‌کند و دارای یک ویرایشگر آنلاین کد است. امروزه امکان همکاری اعضای یک سازمان با یکدیگر از راه دور (ریموت) جزو ضرورت‌ها محسوب می‌شود، و بر این اساس شرکت‌های مهم و معتبری همچون Salesforce، Atlassian و Soundcloud از خدمات Cloud۹ استفاده می‌کنند.

روبن دانیلز (Reuben Daniels) موسس Cloud۹ با ابراز خرسندی از این که شرکت متبوع وی توسط آمازون خریداری شده است گفت این معامله ممکن است بر سیستم قیمت‌گذاری محصولات Cloud۹ تاثیر بگذارد ولی فعلاً همان نرخ‌های قبلی اعمال می‌گردد. سرویس‌های Cloud۹ بر اساس مدل تجاری فری میوم (Freemium) ارائه می‌شود و ماهانه ۱۹ و ۲۹ دلار به ازای هر کاربر هزینه در بر دارد.

درآمد فصلی ۴.۳ میلیارد یورویی SAP از فروش نرم افزار و خدمات ابری

Microsoft



شرکت SAP گزارش داد فروش نرم افزارهای پردازش ابری آن همچنان سیر صعودی را دنبال می کند و البته پس از خروج بریتانیا از اتحادیه اروپا، برخی شرایط ناپایدار برای آنها به وجود آمده است. به گزارش وبسایت Zdnet، شرکت SAP اعلام کرد میزان درآمدهای آن از اشتراک پذیری و پشتیبانی کاربران در خدمات پردازش ابری در فصل دوم از سال مالی جاری با رشد ۳۰ درصدی نسبت به مدت مشابه سال گذشته به رقم ۷۲۰ میلیون یورو رسیده است. مشتریان جدید خدمات پردازش ابری در این شرکت با رشد ۲۸ درصدی درآمدی بالغ بر ۲۵۵ میلیون دلار را به همراه داشته اند. این شرکت توضیح داد: «گسترش سریع خدمات پردازش ابری و پشتیبانی از آن باعث افزایش درآمدها شده است و با این روند میزان درآمدها در آینده را آسان تر می توان پیش بینی کرد». بخش اشتراک در خدمات پردازش ابری SAP و پشتیبانی از آن به همراه بخش پشتیبانی از نرم افزارهای SAP در مجموع ۶۳ درصد از درآمدهای این شرکت در فصل دوم از سال ۲۰۱۶ میلادی را ایجاد کرده است. مجموع درآمدهای SAP در این دوره زمانی ۵.۲ میلیارد یورو محاسبه شد که بخش خدمات پردازش ابری و نرم افزار روی هم رفته ۴.۳۶ میلیارد یورو از آن را به دست آوردند. این رقم رشد ۷ درصدی درآمدهای SAP در این بخش را نشان داد. همچنین گفته شد میزان درآمدهای عملیاتی SAP در این دوره زمانی با رشد ۸۱ درصدی به ۱.۲۷ میلیارد دلار رسیده است.

اوراکل ۲۷۶ حفره امنیتی خود را وصله کرد



آخرین به‌روزرسانی امنیتی اوراکل منتشر شد و طی آن ۲۷۶ نقطه آسیب‌پذیر در نرم‌افزارهای مختلف این شرکت برطرف شد تا کاربران سازمانی با مشکل کمتری روبرو شوند. به گزارش وبسایت Zdnet، بر اساس اطلاعات مندرج در سایت اینترنتی مشاوره امنیتی این شرکت، به‌روزرسانی امنیتی حیاتی (CPU) مربوط به ماه ژوئیه در مجموع مشکلات مربوط به ۸۴ محصول مختلف را برطرف کرده است که از جمله آنها می‌توان به نرم‌افزارهای Java، MySQL، Fusion Middleware، Enterprise Manager و Enterprise Manager اشاره کرد. لازم به ذکر است که شرکت اوراکل طی سال ۲۰۱۵ میلادی در هر به‌روزرسانی خود به‌طور میانگین ۱۶۱ حفره امنیتی را وصله می‌کرد و برای سال ۲۰۱۴ نیز این رقم ۱۲۸ مورد گزارش شده بود. آنچه که وضعیت را برای آخرین به‌روزرسانی دشوارتر می‌کند این است که از بین ۲۷۶ حفره امنیتی وصله شده در ماه ژوئیه، ۱۵۹ مورد به گونه‌ای بودند که به هکرها امکان می‌دادند از راه دور کنترل و مدیریت رایانه را در اختیار بگیرند و بدون اطلاع کاربر به تمام داده‌ها دسترسی داشته باشند. در بسیاری از موارد حملات از طریق شبکه‌های آسیب‌پذیر انجام می‌شد و به هیچ‌تاییدی از جانب کاربران نیاز نداشت. در مجموع ۱۹ مورد از این حفره‌های امنیتی در سیستم امتیازدهی CVSS از عدد ۱۰ رتبه ۹.۸ را دریافت کردند و همین مسئله نشان داد که آنها تا چه اندازه خطرناک بوده‌اند. لازم به ذکر است بیشتر حفره‌های امنیتی وصله شده امتیاز بالای ۹ داشتند.