اهداف فاوای نفت

دستیابی به صنعت نفتی مبتنی بر اندیشه و خرد با محوریت فاوا

ارتقای دانش با محوریت سرمایه فکری به منظور افزایش کارآیی و اثربخشی

ایجاد بسترهای مناسب و مطلوب فاوا جهت دستیابی به صنعت نفت پیشرفته

ارتقاء کارایی و اثر بخشی ارکان مدیریتی و اجرایی از طریق فاوا در صنعت نفت

برنامه‌ریزی و هوشمند سازی فرایندهای کسب‌وکار الکترونیک صنعت نفت

استقرار فراگیر و یکپارچه کاربردها و خدمات فاوا در صنعت نفت

خبرنامه فاوای نفت

فاوای نفت

۳۹۸ شماره خبرنامه ۹۶/۰۵/۱۸ تاریخ انتشار

در این شماره می خوانید:

خبرنامه فاوای نفت از علاقه‌مندان در خصوص ارائه مطالب و پیشنهادات دعوت به مشارکت می نماید

حفره امنیتی در کمین یک میلیارد موبایل

اگر تازه ترین وصله های امنیتی را برای سیستم عامل گوشی خود بارگذاری نکرده اید، بهتر است همین الان این کار را انجام دهید تا از سرقت اطلاعات تلفن همراه خود جلوگیری کنید. محققان موفق به شناسایی آسیب پذیری خاصی موسوم به Broadpwn در تراشه وای فای که در بیش از یک میلیارد گوشی هوشمند موجود در جهان به کار رفته، شده اند.متخصصان شرکت کننده در کنفرانس امنیتی بلاک هت در لاس وگاس آمریکا می گویند هکرها با سواستفاده از مشکل یاد شده می توانند به گوشی های هوشمند افراد نفوذ کرده و کنترل آنها را در دست بگیرند. از تراشه وای‌فای برای اتصال گوشی ها به شبکه های بی سیم استفاده می شود.هکرها می توانند از گوشی هایی که به این شیوه هک شده اند به عنوان ابزار دسترسی و حمله به دیگر گوشی های مجاور استفاده کنند و آنها را به یک کرم هکر وای‌فای مبدل کنند.نکته نگران کننده این است که کاربران گوشی های هک شده به هیچ وجه از موفقیت این حمله مطلع نمی شوند و هیچ اختلالی در استفاده آنها از گوشی ایجاد نمی شود.بررسی ها نشان می دهد که تقریبا تمامی گوشی های ساخت شرکت های مشهور اعم از اپل، اچ تی سی، ال جی، گوگل و ... از تراشه های وای – فای خانواده Broadcom BCM۴۳xx استفاده می کنند که دارای حفره امنیتی مذکور است. محققان می گویند این امر ضرورت توجه به ایمن سازی سخت افزارهای نصب شده بر روی گوشی ها را دوچندان می کند.کاربرانی که از آیفون با سیستم عامل iOS ۱۰.۳.۳ استفاده می کنند و همچنین کاربرانی که وصله های امنیتی ماه جولای اندروید را بر روی گوشی های خود نصب کرده اند، از این مشکل در امان هستند.

مایکروسافت به بنیاد محاسبات بومی ابری پیوست

به‌تازگی شرکت مایکروسافت اقدام به انجام مشارکتی ویژه در زمینه محاسبات و خدمات ابری نموده و در همین راستا به عضویت «بنیاد محاسبات بومی ابری» درآمده است. به نقل از وب‌سایت خبری تحلیلی **cloudcomputing**، بنیاد محاسبات بومی ابری (**CNCF**) یک بنیاد وسیع و بسیار ویژه در زمینه ارائه سرویس محاسبات و دیگر خدمات در فضای ابری بوده که از مشارکت و همکاری چندین شرکت بزرگ فناوری شکل گرفته است.گفتنی است که نام‌های حاضر در فهرست اسامی عضو این بنیاد، هر یک به‌تنهایی یک غول تمام‌عیار در صنایع مختلف دنیای فناوری اطلاعات به‌حساب می‌آیند. شاید کافی باشد صرفاً به دو نام بزرگ و مشهور بسنده کنیم، یعنی دو شرکت «گوگل» و «آی‌بی‌ام».

مطابق تعریف فلسفه وجودی این بنیاد، اهداف آن بدین ترتیب اعلام شده است: ایجاد و ارائه مدل تطبیقی و یک الگوی محاسباتی جدید، که برای محیط‌های سیستم‌های توزیع، بهینه‌سازی شده و قابلیت مقیاس‌پذیری تا ده‌ها هزار گره خودترمیم‌شونده با معماری **multi-tenant** را داراست. اخیراً و در تازه‌ترین تحول مربوط به این نهاد، این بنیاد، یک شریک بسیار نیرومند را در کنار خود می‌بیند. غول نرم‌افزاری جهان، شرکت مایکروسافت، به‌تازگی با هدف پیوستن به این بنیاد، به سراغ آن رفته است تا در یک همکاری ویژه بتواند با این بنیاد در زمینه خدمات ابری جدید فعالیت مشترک داشته و ایده‌ها و سرویس‌های تازه‌ای را طراحی و اجرا نماید.

گوگل حریم شخصی خریداران آنلاین را نقض می‌کند؟

گوگل در ماه می گذشته ابزار جدیدی به نام برآورد خرید از فروشگاه‌ها عرضه کرد که اطلاعات مربوط به خرید کاربران در دنیای واقعی با استفاده از کارت‌های اعتباری را جمع آوری می‌کند. گوگل مدعی است هدف از جمع آوری این اطلاعات نمایش تبلیغات مرتبط با سلیقه و علائق هر خریدار است. اما یک گروه مدافع حریم شخصی معتقد است که این کار گوگل در عمل به جمع آوری اطلاعات جزئی از خریداران کالاهای مختلف منجر می شود و از کمیسیون فدرال تجارت آمریکا خواسته تا این موضوع را به طور جدی پیگیری کند.

گروه اپیک (مرکز اطلاعات و حریم شخصی الکترونیک) در نامه خود خطاب به کمیسیون مذکور تصریح کرده که ابزار گوگل برای ردگیری وبگردی های کاربران قابل استفاده است و در زمان خرید آنلاین جزئی‌ترین اطلاعات مربوط به هر فرد را جمع آوری می کند.در ادامه این نامه آمده است گوگل اطلاعات مذکور را مخفی نگه می دارد و ممکن است آنها را در اختیار شرکت‌های تجاری و فروشگاه های آنلاین قرار دهد و از این طریق حریم شخصی افراد را نقض کند.در نامه اپیک آمده اگر چه در تنظیمات حساب کاربری ابزار یاد شده امکاناتی برای کاهش افشای اطلاعات خصوصی خریداران وجود دارد، اما به نظر می رسد که اطلاعات کارت‌های اعتباری افراد حتی بعد از تنظیم محدودیت ها در بخش تنظیمات توسط گوگل افشا شود و ضروری است گوگل در این زمینه به طور شفاف و واضح واکنش نشان دهد.

در این نامه خواسته شده تا گوگل برای افشای اسامی شرکت های تجاری که در همین راستا با آنها همکاری می کند تحت فشار قرار گیرد. گوگل در واکنش گفته که حفظ حریم شخصی کاربران را جدی تلقی می کند و به طور کامل اتهامات وارده را مردود می داند.

اطلاعات مرورگرها به‌راحتی قابل شنود است

تحقیقات جدید محققان امنیتی نشان داده است که استفاده از شبکه اینترنت به کمک مرورگرها، آنچنان که پیش‌تر تصور می‌شد امن نیست، بلکه می‌توان گفت تقریباً به‌راحتی توسط دولت‌ها و هکرها قابل شنود هستند.به نقل از وب‌سایت خبری تحلیلی **theinquirer**، گروهی از محققان امنیتی آلمانی به‌تازگی در پی تحقیقات خود به این نتیجه رسیده‌اند که امروزه دستیابی به اطلاعات مرورگر افراد، حتی در صورتی که استفاده از سیستم وب‌گردی را به‌صورت ناشناس انجام دهند نیز بسیار آسان است.گفتنی است این محققان توانستند اطلاعات مربوط به وب‌گردی سه میلیون شهروند آلمانی را با استفاده از روش رهگیری اطلاعات **clickstream** جمع‌آوری کنند.

اطلاعات **clickstream** معمولاً توسط صنایع تبلیغات با هدف کاربرهای خاص و بر اساس تجربیات وب‌گردی آنها مورد استفاده قرار می‌گیرد. پیش از این تصور می‌شد که اطلاعات به دست آمده از این طریق باید ناشناس باشند، اما این محققان اکنون دریافته‌اند که دور زدن این اقدام امنیتی نیز بسیار آسان است و انجام آن می‌تواند اطلاعات بسیار حساس کاربران خاصی را افشا سازد.علاوه بر این، زمانی که این اطلاعات با اطلاعات عمومی گره خورده باشند (مانند لینک‌هایی که افراد بر روی توئیتر به اشتراک می‌گذارند یا عکس‌هایی که بر روی صفحه فیس‌بوک خود آپلود می‌کنند) می‌توان به‌راحتی آنها را به فردی مشخص مربوط ساخت.این گروه همچنین با انجام این کار ثابت کردند که دست‌یابی به اطلاعات افراد با روش **clickstream** –که بسیار متداول نیز هست– غیرقانونی بوده و افرادی که این کارها را انجام می‌دهند می‌توانند از این اطلاعات به‌راحتی سوءاستفاده کنند.لازم به ذکر است که خود افراد این گروه پس از انجام تحقیقات خود اطلاعات به‌دست‌آمده را کاملاً پاک کردند، زیرا خودشان نیز از هک شدن و قرارگیری این اطلاعات در دست افراد نادرست می‌ترسیدند.

کارت شبکه ۱۰ گیگابیتی سازگار با چند استاندارد اترنت

ایسوس به‌تازگی کارت شبکه **XG-C۱۰۰C** را در نوع **PCIe** معرفی کرده است که در اصل برای شبکه‌های ده گیگابیتی طراحی شده، اما با استفاده از فناوری **Aquantia** می‌تواند استانداردهای جدید شبکه‌های **۱۰ Gbps**، **۵ Gbps**، **۲,۵ Gbps**، **۱ Gbps** و درنهایت **۱۰۰ Mbps** را هم پشتیبانی کند و به این ترتیب برای چند استاندارد و نوع شبکه کاربری دارد. این کارت شبکه روی اسلات توسعه **PCIe ۳,۰** با سرعت **۴X** نصب می‌شود و از درگاه **RJ۴۵** و کابل‌های اترنت رایج **Cat۵e/Cat۶** پشتیبانی می‌کند. این کارت شبکه فقط یک درگاه **RJ۴۵** روی برد کنترلر **Aquantia AQtion AQC۱۰۷** دارد و با استفاده از چراغ **LED** می‌تواند سرعت شبکه را گزارش کند. برای راحتی در نصب و استفاده کاربران، از انواع کامپیوترهای دسکتاپ مبتنی بر ویندوز ۱۰ یا لینوکس با نسخه هسته ۴.۴ پشتیبانی می‌کند. روی برد نسبتاً کوچک این کارت شبکه، یک خنک‌کننده آلومینیومی استفاده شده تا در هنگام اوج بار کاری در کامپیوترهای مخصوص بازی یا دستگاه‌های ایستگاه کاری و سرور مشکلی پیش نیاید. قیمت این کارت شبکه ۱۰۰ دلار است و از ماه ژوئن وارد بازار شده است.

رفع قیلتر یوتیوب در دانشگاه‌ها

معاون وزیر ارتباطات و فناوری اطلاعات از اعلام شرایط رفع فیلتر یوتیوب و بلاگ‌اسپات در دانشگاه‌ها با نظر دادستان کل کشور خبر داد.
محمدجواد آذری جهرمی در صفحه اینستاگرام خود، با اشاره به پیگیری برای رفع فیلتر دو سرویس اینترنتی برای کاربران دانشگاهی نوشت: امروز پس از پیگیری‌های انجام‌شده در خصوص رفع فیلتر یوتیوب و بلاگ‌اسپات در دانشگاه‌ها، با نظر مساعد دادستان محترم کل کشور، شرایط رفع فیلتر این سرویس‌ها در دانشگاه‌های کشور طی نامه‌ای به ما اعلام شد.وی همچنین خاطرنشان کرد: تلاش می‌کنیم برای پیاده‌سازی شرایط اعلامی تسریع به عمل آید.گفتنی است ماه گذشته بود که آذری جهرمی از رایزنی با دادستانی کل کشور برای رفع فیلتر دو سرویس بلاگ‌اسپات و یوتیوب در جهت درخواست‌های مجموعه دانشگاهی سخن گفته بود و زمان آن را به تصمیم کارگروه فیلترینگ موکول کرده بود.مدیرعامل شرکت ارتباطات زیرساخت همچنین درباره شرایط رفع فیلتر این سرویس‌ها اظهار کرده بود: موضع دادستانی این است که اگر ما به عنوان مجری بتوانیم نظام کنترل خطوط قرمز را پیاده‌سازی کرده و در کنار هم قرار دهیم، مخالفتی با این مساله نخواهند داشت. با توجه به این که برخی از این سایت‌ها به صورت رمزی هستند و قابلیت فیلترینگ هوشمند ندارند، این کار شاید در قالب مذاکره با سرویس‌دهنده یا استفاده از راهکارهای دیگری انجام شود.