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

۴۰۸ شماره خبرنامه ۹۶/۰۸/۰۳ تاریخ انتشار

در این شماره می خوانید:

بزرگ‌ترین تحول چهار دهه اخیر شبکه‌های کامپیوتری

از SDN به عنوان بزرگ‌ترین تحول چهار دهه شبکه‌های کامپیوتری نام برده می‌شود. SDN برای اولین بار در سال ۲۰۰۵ مطرح شده و از سال ۲۰۱۰ شتاب گرفت و در سال ۲۰۱۱ با تشکیل بنیاد ONF و عضویت بیش از هشتاد شرکت بزرگ صنعت شبکه در آن و تدوین استاندارد OpenFlow وارد فاز جدیدی شد. اولین محصولات SDN در سال ۲۰۱۲ و بیشتر ۲۰۱۳ وارد بازار شده و پیش‌بینی می‌شود تا آینده این نوع شبکه‌ها کم‌کم جایگزین شبکه‌های سنتی مبتنی بر اترنت و TCP/IP شوند. شبکه تعریف شده‌ی نرم افزاری (Software-Defined NetworkingSDN)یک تکنولوژی جدید است که می تواند در طراحی و مدیریت بر شبکه، نوآوری داشته باشد اگر بخواهیم شبکه‌های نرم‌افزار محور یا SDN را خیلی ساده تعریف کنیم باید بگوییم: «نسل جدیدی از شبکه‌ها که با استفاده از لایه‌های مجازی، سوییچ‌های مجازی، کنترلر مرکزی، استانداردهای ارتباطی و API های سطح بالا سعی می‌کنند برخی از کارهای کنترلی و مدیریتی سوییچ‌ها و روترهای شبکه را در لایه‌های بالاتر به صورت نرم‌افزاری انجام دهد». به زبان دیگر SDN وابستگی به سخت‌افزار را کاهش داده و قابلیت‌های نرم‌افزاری و هوشمندی شبکه را افزایش می‌دهد.هر یک تجهیزات شبکه به شکل و ساختار خود پیکربندی می‌شود و هر کدام باید بصورت جداگانه مورد پیکربندی قرار گیرد، حال اگر شبکه با وسعت شبکه یک کشور داشته باشیم که از هزاران سویچ و روتر تشکیل شده، تقریباً کار بسیار سخت و زمان بری خواهد بود و چگونه می‌توان عدم بروز خطا را گارانتی نمود. به چند نفر و چند ساعت کار برای پیاده‌سازی یک تغییر کوچک که اتفاقاً باید در تمامی تجهیزات اعمال شود نیاز است.پس در همین جا نیاز به یک سیستم یکپارچه کننده شبکه احساس می‌گردید. سیستمی که بتواند فراتر از هر پروتکل و پیچیدگی کار کاربران و مدیران شبکه را کم و به بهترین شکل پیاده سازی کند. سیستمی که در واقع بتواند دستورات را از کاربر گرفته و به زبان و کدهای مختلف کامپایل کرده و به تجهیزات اعمال کند فارغ از هرگونه درگیر شدن کاربر و یا حتی اطلاع آن از پیچیدگی و تنوع شبکه.

در اینجا نیاز به یک مجازی‌سازی بر روی سخت افزارهای شبکه حس می‌گردید به شکلی که اجزاء شبکه بصورت منابع تحت کنترل قرار گیرند و همانند پردازنده و حافظه قابل مدیریت و برنامه ریزی باشند. بتوان این اجزا را در یک محیط مجازی تحت کنترل قرار داد. یک شبکه مجازی که اجزاء آن را منابعی همانند سویچ‌ها، روترها و تجهیزات شبکه تشکیل می‌دهند و براحتی می‌توان آنها را برنامه ریزی کرد. براحتی می‌توان یک کد را از طرف کاربر گرفته و به شبکه مجازی اعمال نمود.

گزارش سالانه گوگل از ترافیک و امنیت وب

چند سالی است که گوگل اصرار زیادی دارد که وبسایت‌ها وسرویس‌های اینترنتی سراسر دنیا از پروتکل **HTTPS** استفاده کنند. چرا که در این پروتکل تمامی اطلاعات رد و بدل شده بین مرورگر کاربر و وبسایت تماما به‌صورت رمزگذاری شده و محفوظ رد و بدل می‌شود. با استفاده از این پروتکل، کاربران اینترنت می‌توانند خودشان را در مقابل افرادی که قصد دستکاری دیتا را دارند، محافظت کرده و خطر لو رفتن اطلاعاتشان در دنیایی که حتی نمی‌توان به سیستم وای‌فای هم اعتماد کرد را تا مقدار قابل توجهی کاهش دهند. گوگل در گزارش سالانه جدید خود اعلام کرده که ۸۹ درصد از محصولات و سرویس‌های این شرکت در حال حاضر از پروتکل **HTTPS** استفاده می کنند. این آمار در سال ۲۰۱۴ کمتر از ۵۰ درصد بود. تعداد ۱۰۰ وبسایت برتری که از سیستم **HTTPS** استفاده می‌کنند نیز از پارسال تا به امروز از ۳۷ به ۷۱ وبسایت افزایش پیدا کرده است.

حال که اکثر سرویس‌های متعلق و وابسته به گوگل از پروتکل استفاده می‌کنند، برنامه‌نویسان هم حالا دلایل و تمایل بیشتری برای تغییر سرویس‌هایشان و پیوستن به این پروتکل دارند. گوگل ادعا می‌کند امروزه بیش از ۳۷ درصد وبسایت‌هایی که در کشور آمریکا و از طریق مرورگر کروم این شرکت جستجو می‌شوند، به صورت رمزگذاری شده (**HTTPS**) نمایش داده می‌شوند. یکی از دلایلی که از رشد وبسایت‌ها و محتوا به شکل رمزگذاری شده جلوگیری می‌کند، تلفن همراه‌های قدیمی هستند که به دلیل قدیمی بودن سخت‌افزارهایشان نمی‌توانند از این نوع پروتکل‌ها پشتیبانی کنند.

حجم دیتای تولیدی دنیا به ۱۸۰ زتابایت می رسد

رئیس پژوهشگاه ارتباطات و فناوری اطلاعات گفت: تا سال ۲۰۲۵ حجم دیتای تولیدی در دنیا به حدود ۱۸۰ زتابایت (zeta byte) می‌رسد و لذا مقررات گذاری برای استفاده «بیگ دیتا» در کشور در حال انجام است. محمدخوانساری گفت: با توجه به ارزش دیتا در قرن ۲۱ و نیروی محرکه ای که داده‌ها برای اقتصاد دنیا ایجاد می‌کنند، به زودی اطلاعات قطعا جایگزین نفت شده و به طبع آن رشد اقتصادی، زیرساخت‌های جدید و کسب وکارهای نو، همگی وابسته به دیتا می‌شود.وی گفت: پیش بینی انجام شده این است که تا سال ۲۰۲۵ حجم دیتای تولیدی در دنیا در حدود ۱۸۰ زتابایت (zeta byte) می‌شود و لذا ما ملزم به پالایش این حجم عظیم دیتا می‌شویم.

خوانساری با تاکید به اینکه در حال حاضر حجم بالایی از دیتا از طریق دستگاه‌های شخصی مردم در حال خروج از کشور است ، خاطر نشان کرد: این درحالی است که دیتا با ارزش ترین منبع جهان می شود؛ بنابراین هم در دولت و هم در بخش خصوصی باید در این راستا اقداماتی برای از بین بردن انحصار شرکتهای بزرگ دنیا مانند گوگل صورت گیرد. وی بر اهمیت پردازش دیتا در داخل کشور تاکید کرد و افزود: اگر ما نتوانیم تجمیع و پردازش دیتا را در داخل کشور انجام دهیم، اشتغال این حوزه به خارج از کشور می رود و به همین منظور در دولت و در وزارت ارتباطات و فناوری اطلاعات، در حال بررسی بحث رگولاتوری «بیگ دیتا» و تنظیم مقررات «داده‌های کلان» هستیم.رئیس پژوهشگاه ارتباطات وفناوری اطلاعات، اضافه کرد: کشورهایی که در حال تولید دیتا خام و عرضه رایگان آن هستند، باعث به وجود آمدن فاصله دیجیتالی میان کشورها می‌شوند. رئیس مرکز تحقیقات مخابرات ایران با بیان اینکه در قدم بعدی باید مسیری را انتخاب کنیم که باعث کاهش فاصله دیجیتالی کشورمان از کشورهای دیگر شود، گفت: در واقع فاصله دیجیتالی میان کشورها ناشی از عدم پردازش داده‌ها است که باعث وابستگی به خارج و تسلط محتوایی بر کشور و مردم می شود.

تروجان‌های جدید گوگل از تمامی جنبه‌های زندگی

به گزارش شبکه خبری **ICTPRESS**، گوگل قصد ندارد به سامسونگ یا اپل دیگری مبدل شود و به جای این کار بخش سخت افزاری گوگل به دنبال استفاده از فناوری هوش مصنوعی به منظور کنترل جزئی ترین بخش های حیات بشری است.گوگل برای افزایش توانمندی خود در حوزه سخت افزار به دنبال خرید واحد تولید گوشی های هوشمند شرکت اچ تی سی نیز بوده و بدین منظور قصد دارد یک میلیارد دلار هزینه کند.این شرکت تا چندی قبل بخش عمده درآمد خود را از محل تبلیغات آنلاین به دست می آورد، اما این وضعیت به زودی تغییر خواهد کرد و گوگل محصولات هوش مصنوعی جدیدی عرضه می کند که از توانمندی های بی سابقه ای برای جمع آوری اطلاعات برخوردارند. به نظر می رسد ارتقای دستیار صوتی گوگل هوم و تلاش برای افزودن آن به طیف گسترده ای از محصولات و خدمات به همین منظور صورت می گیرد. اضافه شدن هوش مصنوعی به گوشی های اندرویدی، لوازم خانگی و غیره به گوگل امکان خواهد داد تا کنترل بی سابقه ای بر زندگی شخصی و حرفه ای انسان ها پیدا کند و امپراطوری خود را بیش از پیش تکمیل کند.

یکی از محصولات جدید گوگل که با همین رویکرد تولید شده دوربین تازه آن به نام گوگل کلیپس است که از هوش مصنوعی برای کنترل اتفاقات محیط اطراف و تعیین بهترین زمان برای تهیه کلیپ های ویدئویی کوتاه استفاده می کند. سپس این کلیپ ها به سرویس عکس گوگل منتقل می شوند و از فناوری تشخیص چهره به منظور ارتقای دائمی کارکرد این خدمات استفاده می شود.گوگل از فناوری هوش مصنوعی در گوشی های بی سیم **Pixel Buds** خود نیز استفاده کرده که برای ترجمه آنی مطالب استفاده می شوند. انتظار می رود این قابلیت در بسیاری از محصولات گوگل به کار گرفته شود. با این حساب گوگل در آینده به حجمی بی سابقه و کم نظیر از اطلاعات خصوصی میلیاردها نفر از ساکنان کره زمین دسترسی می یابد.

سه خطر امنیت سایبری که باید از آن آگاه بود.

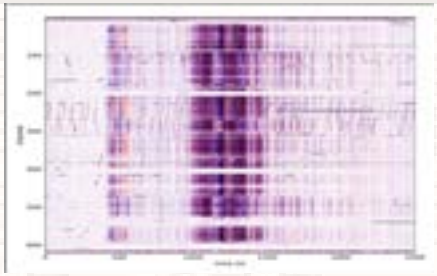
درحالی که پیش بینی اینکه آینده جرایم سایبری به کجا منجر خواهد شد ، مشکل است ، چند گرایش ویژه وجود دارد که باید مورد توجه قرار گیرند، در این مطلب به سه گرایش اصلی آن می‌پردازیم .

۱– کارکنان امنیتی که به طور جدی متضرر شده اند: پوشیده نیست که نیرو های امنیت سایبری با سرعت کافی نمیتوانند رشد کنند تا به نیازهای بازار برسند. یک تحقیق جدید نیروی اطلاعات امنیتی جهانی ۲۰۱۷ برآورد می کند که تا سال ۲۰۲۲، بیش از ۱،۸ میلیون مو قعیت در حوزه امنیت سایبری خالی خواهد ماند.

۲– باج افزارها : اگر چیزی وجود دارد که در سال ۲۰۱۷ باید به آن فکر کنیم، این است که باج افزارها به سرعت در حال تبدیل شدن به یکی از خطرناکترین تهدیدات در جهان امنیت سایبر است. حمله ی باج افزار **WannaCry** دربهار ۲۰۱۷ شروع شد و بیش از ۳۰۰،۰۰۰ کامپیوتر در بیش از ۱۵۰ کشور مختلف را تحت تاثیر قرار داد.درحالی که **wannaCry** قطعا یکی از حملات تروریستی ویرانگر است که جهان تا به حال دیده است، قطعا تنها نیست. در واقع، **Cybersecurity Ventures** گزارش می‌دهد که هزینه‌های خسارت ناشی از خرابکاری جهانی باج افرار ها در سال ۲۰۱۷ به بیش از ۵ میلیارد دلار برسد که ۱۵ برابر بیشتر از ۳۲۵ میلیون دلار در سال ۲۰۱۵ است.این بدون شک یک آمار دقیق برای بسیاری است، به ویژه از آنجا که تنها در حدود یک در پنج مدیر اجرایی جهانی به طور کامل اطلاعات را به استراتژی و برنامه ریزی کلی آنها اضافه می کنند.از همه این‌ها این است که امنیت سایبری بدون شک باید یکی از اولویت‌های اصلی تصمیم گیرندگان در سطح اجرایی باشد.با این وجود، گام‌های به خصوص سادهای که میتوانید انجام دهید (بسیاری از آنها زمان و تلاش بسیار کم) برای جلوگیری ازحملات **ransomware** وجود دارد.

۳– غفلت کارمندان : در نهایت، یکی از سختترین تهدیدات در کسب و کار امروز، مربوط به کارمندان شما است. در حقیقت، اکثریت قریب به اتفاق (۶۰٪ با توجه به گزارش امنیت اطلاعات سایبر آی بی ام ۲۰۱۶) نقص امنیتی در واقع به طور مستقیم توسط کارکنان ایجاد میشود. اینکه آیا دریک تله فیشینگ گیر می‌کنید، اتصال به وای فای‌های خطرناک ، ایجاد برنامه‌های خطرناک دردستگاه‌های خود و یا عدم پیروی از استانداردهای امنیتی اولیه، یک کارمند بیاطلاع میتواند تعدادی از بکدورها برای مهاجمان سایبری را باز کند وموجب ضررمیلیونی کسب و کار خود گردد.

کشف زلزله با استفاده از کابل فیبر نوری



به گزارش شبکه خبری **ICTPRESS**، در زمان وقوع زلزله هر چقدر هشدار آن فاصله زمانی بیشتری با وقوع زلزله داشته باشد، بهتر است. دستگاه‌های زلزله‌نگار موجود فعلی برد کوتاهی داشته و قیمت آنها نیز بالاست، اما محققان دانشگاه استنفورد آمریکا موفق شدند با استفاده از کابل‌های فیبر نوری یک شبکه اعلام هشدار زلزله بسازند که می‌تواند در سراسر شهر گسترده شود.با توجه به اینکه اساس کار فیبر نوری بر پایه حرکت امواج نوری در یک محیط شیشه‌ای است، اختلالات جزئی در سیگنال‌های آن نیز قابل اندازه‌گیری است و این فناوری در صنعت نفت و گاز در حال حاضر مورد استفاده قرار می‌گیرد.«آیلین مارتین»(**Eileen Martin**) یکی از محققان ارشد این پروژه گفت: همان‌طور که در زمینه نفت و گاز این سامانه زمانی که با آلودگی‌های گوناگون مواجه می‌شود، سیگنال را برمی‌گرداند، در کشف لرزه نیز زمانی که فیبرها شروع به کشیده شدن در بعضی مناطق می‌کنند، در سیگنال آنها تغییر ایجاد می‌شود.

برای بررسی این موضوع که آیا این کابل‌ها می‌توانند برای پیش‌بینی و اندازه‌گیری زلزله مورد استفاده قرار بگیرند، محققان در زیر سطح دانشگاه استنفورد کابل‌های فیبر نوری به طول ۴,۸ کیلومتر را به شکل ۸ قرار دادند تا با استفاده از پرتوهای لیزر به ضبط حرکات احتمالی بپردازند. این شبکه فعالیت خود را از سال ۲۰۱۶ آغاز کرده است و در یک سال گذشته موفق به ثبت بیش از ۸۰۰ مورد لرزه طبیعی و مصنوعی شده است.این شبکه موفق شده است علاوه بر تشخیص لرزه‌های ناشی از انفجارها و آزمایش‌های نظامی، زلزله ۸,۲ ریشتری اخیر در مکزیک را از فاصله ۳۲۲۰ کیلومتری تشخیص دهد.با وجود دستاوردها و نتایج امیدوارکننده کابل‌های فیبرنوری محققان اعلام کرده‌اند که سامانه‌های معمول فعلا در کشف امواج بهتر عمل می‌کنند، اما مزیت این سامانه قیمت ارزان و قابلیت رساندن و پخش کردن آن در سراسر شهرهاست.هر متر از این کابل‌ها به منزله یک حسگر زلزله عمل می‌کند که با هزینه‌ای کمتر از یک دلار نصب می‌شود و امکان پیاده‌سازی چنین شبکه‌ای با استفاده از لرزه‌نگارهای معمول وجود ندارد.نتایج این تحقیق در نشریه **SEG Technical Program Expanded Abstracts** ۲۰۱۷ منتشر شده است.