



خبرنامه فاوای نفت



تاریخ انتشار: ۹۶/۰۹/۲۲ شماره خبرنامه: ۴۱۴

مأموریت: مدیریت، بازاریابی، بازرسی، نگهداری و تعمیرات، ایمنی، بهداشت، محیط زیست، منابع انسانی، مالی، فناوری اطلاعات، بازاریابی، بازرسی، نگهداری و تعمیرات، ایمنی، بهداشت، محیط زیست، منابع انسانی، مالی، فناوری اطلاعات



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
برنامه ریزی و هوشمند سازی فرایندهای کسب و کار الکترونیک صنعت نفت
استقرار فراگیر و یکپارچه کاربردها و خدمات فاوا در صنعت نفت



اپلیکیشن



سایت



امنیت



آپدیت

در این شماره می خوانید:

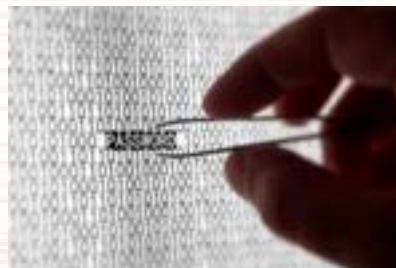
backup server

- رمز عبور
- تلگرام
- قفل آیفون
- سرعت دانلود



علی‌رغم گوشزدها و توصیه‌های شرکت‌های ارائه دهنده خدمات راه اندازی backup server مبنی بر پیاده سازی تجهیزات ذخیره ساز SAN & NAS و نرم افزار بکاپ گیری تحت شبکه، متأسفانه اغلب مدیران شرکت‌ها و سازمان‌ها این توصیه‌ها را جدی نگرفتند و در دام باج افزارها گرفتار شدند. در واقع عدم رغبت مدیران شرکت‌ها به راه اندازی backup server، موجب آسیب پذیری شبکه‌های کامپیوتری سازمان به تهدیدات علیه امنیت اطلاعات سازمان و در نهایت منجر به پرداخت باج‌های سنگین به بدافزارها شد. در صورتی که مدیران با هزینه‌های بسیار کمتر از خسارت‌های وارد شده، تنها از طریق راه اندازی backup server می‌توانستند بدون پرداخت هزینه‌های سنگین به باج افزارها، اطلاعات سرور و یا کامپیوترهای خود را به سادگی بازیابی کنند. گسترش پیدا کردن موج گرفتار شدن کسب‌وکارها و سازمان‌ها به بدافزارها موجب شد که شرکت‌ها به کمک راه اندازی backup server به فکر امنیت اطلاعات کامپیوترهای خود نیز باشند! گرچه اقدام آنها برای پیاده سازی بکاپ گیری از سرور، نوش دارو پس از مرگ سهراب تلقی می‌شود اما به هر حال، بکاپ گیری سرور از طریق شبکه می‌تواند موجب بیمه شدن دیتاهای سازمان در حملات سایبری آتی باشد. چراکه خبرها حاکی از آن است که روزانه باج افزارهای جدیدی تولید می‌شوند و هر لحظه این امکان وجود دارد آن دسته از شرکت‌هایی که اعتقادی به راه اندازی backup server نداشتند و گرفتار باج افزارها شدند، دوباره مورد حمله قرار بگیرند و اطلاعات خود را از دست بدهند.

عدم تمایل بسیاری از شرکت‌ها به به کاپ گیری از سرور و خسارت دیدن سازمان‌ها ناشی از باج افزارها، باعث شد سازمان‌ها و شرکت‌های دیگر درس عبرت بگیرند و به فکر راه اندازی backup server برای ایمن سازی اطلاعات سرورهای خود باشند. اگر شما نیز صاحب شرکت و یا کسب‌وکاری هستید که از کامپیوترها در سازمان خود استفاده می‌کنید، می‌بایست هرچه سریع‌تر نسبت به امنیت اطلاعات در کامپیوترهای خود به وسیله خدمات راه اندازی backup server شرکت‌های فعال و معتبر در حوزه شبکه، اقدام کنید. کاربران خانگی که طبیعتاً با حجم اطلاعات کمتری سروکار دارند، می‌توانند از خدمات سرویس‌های آنلاین برای پشتیبان گیری دیتاهای خود استفاده کنند. اما شرکت‌ها و سازمان‌ها می‌بایست حتماً توجه ویژه‌ای برای راه اندازی backup server قائل باشند و از این طریق امنیت اطلاعات سرورهای شرکت خود را در برابر حملات باج افزارها حفظ کنند.



مدیریت رمز عبور بسیار مشکل است. به طور معمول، سایت‌های خرید و برنامه‌های بسیار زیادی وجود دارند که هر کدام رمز عبور مخصوص به خود را داشته و به همین خاطر، مدیریت این تعداد زیاد از رمز عبور، کار دشواری به نظر می‌رسد. اگر نگاهی گذرا به متداول‌ترین رمزهای عبور سال ۲۰۱۶ بیندازید، به وضوح می‌بینید که رمز «۱۲۳۴۵» کاربرد بسیار زیادی داشته است. البته «۱۲۳۴۵۶۷۸۹» هم در بسیاری از مواقع مورد استفاده قرار می‌گیرد. بر اساس نظرسنجی جدیدی که از ۶۰۰ نفر به عمل آمده است، ۳۷ درصد افراد بر این باور بودند صرفاً زمانی که سایت از آنها درخواست می‌کند، رمز عبور خود را تغییر می‌دهند. همچنین یازده درصد از این افراد اذعان داشتند که حداقل هفت سال است که رمز عبور خود را تغییر نداده و در تمام این مدت، از یک رمز عبور ثابت استفاده نموده‌اند. عجیب است، تعداد افرادی که رمز عبور خود را تغییر نمی‌دهند، تا این حد پایین است. این احتمال وجود دارد که مردم دارند متوجه خطرات شده و اخبار موجود در مورد هک‌ها و مهاجمان سایبری، ذهن آنها را برای تغییرات لازم آماده نموده که البته اتفاق بسیار خوبی است. یکی از نتایج جالب این نظرسنجی این بود که تمایل مردان به استفاده از واژه «password» به عنوان رمز عبور، ۲٫۸ برابر بیشتر از زنان است. زنان تمایلات دیگری برای استفاده از رمز عبور از خود نشان داده‌اند. نظیر اینکه، تمایل آنها برای استفاده از نام همسرشان به عنوان رمز عبور، ۱٫۳ برابر مردان بود. بسیاری از افراد حاضر در نظرسنجی، اذعان داشتند که در سایت‌ها و برنامه‌های مختلف، از رمز عبور واحدی استفاده می‌کنند. با همه این وجود، کارشناسان امور امنیتی معتقدند که حفظ امنیت، تنها و تنها با داشتن رمز عبور نیست که حاصل می‌شود، بلکه می‌بایست ملاحظات فنی بیشتری را در نظر داشت. حریم خصوصی، واژه‌ای است که با پیشرفت تکنولوژی، تعریف جدیدی یافته است؛ واژه‌ای وسیع که حفظ آن هم دقت و معلومات خاص خود را طلب می‌کند. حفظ حریم شخصی و یا به تعبیر دیگر، امنیت اطلاعات را از جنبه‌های مختلفی می‌توان بررسی نمود. اما اشتباه نکرده‌ایم اگر رمز عبور را سرباز خط مقدم مقابله با سارقان اطلاعات و هویت بنامیم.



پاول دوروف با ارزش گذاری جدید تلگرام به میزان پنج میلیارد دلار حالا در مصاحبه با بلومبرگ تصویر تازه‌ای از این شبکه اجتماعی موبایلی ارائه داده است. دوروف که هم اکنون دفتر این شرکت را در دوبی تاسیس کرده می گوید قصد فروش تلگرام را ندارد و حتی پیشنهاد ۲۰ میلیارد دلاری هم او را به تسلیم وا نمیدارد. دوروف که در سال ۲۰۱۴ مجبور شد باقیمانده سهام خود در بزرگترین شبکه اجتماعی روسیه موسوم به VK را به یکی از میلیاردرهای دولتی این کشور بفروشد از آن زمان تاکنون بر روی تلگرام متمرکز شده است. به گفته دوروف این شبکه اجتماعی ۱۸۰ میلیون نفر کاربر دارد که تنها ۴۰ میلیون نفر از آنها در ایران زندگی می کنند. وی افزوده که هر روز ۵۰۰ هزار نفر به جمع کاربران تلگرام اضافه می شوند.

وی و برادر مسن ترش نیکولای که ریاضی دانی برجسته و برنامه نویس رایانه است، تلگرام را به تدریج توسعه داده اند و آن را از کشوری به کشور دیگر به پیش می برند. پاول دوروف مدعی است در برابر خواست اف بی آی برای افشای اطلاعات خصوصی کاربرانش مقاومت کرده است. او افزوده اف بی آی برای دسترسی به اطلاعات یادشده تا بدان حد جدی بوده که حاضر شده به یکی از برنامه نویسان تلگرام در سان فرانسیسکو رشوه بدهد. دوروف محل نگهداری سرورهای تلگرام را مخفی نگهداشته و حتی نام بسیاری از کارکنان تلگرام که این روزها میلیونر شده اند، مشخص نیست. تلگرام به تازگی دفتری را در طبقه ۲۳ آسمانخراشی در شهر دوبی تاسیس کرده و قصد دارد در سال ۲۰۱۸ دست به نوآوری های تازه ای بزند. دوروف که روسیه را با ۳۰۰ میلیون دلار پول و ۲۰۰۰ بیت کوین ترک کرده بود این روزها قصد دارد خلاقیت های تازه ای به خرج دهد.



به گزارش شبکه خبری ICTPRESS به نقل از گیزمودو، شکستن قفل گوشی آیفون یا «Jailbreaking» روشی برای بهره گیری از آسیب پذیری های سیستم عامل iOS گوشی مذکور با هدف نصب برنامه های مورد علاقه ولی تایید نشده توسط اپل، تغییر راحت رابط کاربری این گوشی و راه اندازی برنامه های شبیه ساز است که در نسخه های استاندارد سیستم عامل iOS ممکن نیست. اپل همیشه تلاش کرده شکستن قفل سیستم عامل iOS خود را ناممکن کند، اما هر بار هکرها روشی برای دور زدن محدودیت های اعمال شده توسط اپل یافته اند. از زمان عرضه نسخه ۱۰ سیستم عامل یادشده شکست قفل آن هر بار دشوارتر و دشوارتر شده و معمولاً «Jailbreaking» عمومی و سراسری آیفون ممکن نبوده است؛ لذا اعلام خبر یادشده توسط گوگل تحولی قابل توجه محسوب می شود. «یان بیر» مهندسی که موفق به این کار شده می گوید به زودی ابزار لازم برای قفل شکنی آیفون های جدید را نیز برای استفاده تمامی علاقمندان عرضه می کند. وی برای پروژه «زیروی» شرکت گوگل کار می کند که تمرکز آن توجه شناسایی مشکلات و چالش های امنیتی و اطلاع رسانی به توسعه دهندگان و برنامه نویسان در مورد حفره های خطرناک امنیتی است. این افراد معمولاً به شرکت ها و افراد برای حل مشکلات امنیتی شناسایی شده ۹۰ روز مهلت می دهند و در غیر این صورت عموم مردم را در جریان مشکل شناسایی شده قرار می دهند.



شرکت **Synaptics** که سازنده مشهور تجهیزات مربوط به سیستم اثر انگشت و **Trackpad** برای بسیاری از برندهاست اعلام کرده که نخستین سنسور اثر انگشت زیر صفحه نمایش را تولید کرده است. نحوه کار این سیستم اثر انگشت درست شبیه دکمه‌های فعلی است که سنسور اثر انگشت زیر آن قرار گرفته با این تفاوت که حالا با قراردادن اثر انگشت روی صفحه نمایش میتوان اثر انگشت را ثبت کرد. این دقیقاً تکنولوژی است که سالهاست بسیاری به خصوص در داخل شرکتهای سازنده موبایل به آن می‌اندیشیدند چراکه با داشتن آن فضای بیشتری را میتوان به صفحه نمایش اختصاص داد. نام این تکنولوژی **Clear ID** است و احتمالاً بزرگترین سازندگان گوشی از آن استقبال خواهند کرد از جمله اپل، سامسونگ، هواوی، اوپو/ویوو، و شیائومی. شرکت **Synaptics** سابقه همکاری با سامسونگ را در کارنامه خود دارد که ساخت صفحات نمایش **infinity** از آن جمله است که هم اکنون در گلکسی اس ۸ و نوت ۸ به کار رفته است. با این حال گفته می‌شود که سامسونگ قصد دارد تا به همکاری خود با این شرکت در زمینه ساخت این نوع صفحات نمایش خاتمه دهد. هر شرکتی که با **Synaptics** وارد شراکت در ساخت این نوع سنسورها شود قطعاً از این تکنولوژی در محصولات خود بهره خواهد گرفت. از جمله گفته می‌شود که شیائومی یک کاندیدای همکاری در این زمینه است.



Speedtest.net یک خدمت مبتنی بر وب است که تحلیلی رایگان از پارامترهای دسترسی به اینترنت در سراسر جهان فراهم می‌کند. این وب سایت که به شرکت **Ookla** تعلق دارد آگوست گذشته ابزار «شاخص جهانی **Speedtest**» را رونمایی کرد. این ابزار سرعت اینترنت در سراسر جهان را رصد می‌کند. طبق سنجش‌های **Speedtest** سرعت دانلود موبایل جهان طی ۱۲ ماه گذشته ۳۰.۱ درصد و سرعت آپلود موبایل نیز ۳۸.۹ درصد افزوده شده است. این ابزار همچنین نشان داد سرعت دانلود پهنای باند ثابت نیز ۳۱.۶ درصد بهبود یافته است. این در حالی است که متوسط سرعت دانلود موبایل ۲۰.۲۸ و دانلود پهنای باند ثابت ۴۰.۱۱ مگابایت بر ثانیه اعلام شده است.

طبق این شاخص، سرعت دانلود موبایل در ایران ۱۶.۷۴ مگابایت بر ثانیه و سرعت آپلود موبایل **Mbps ۸.۳۷** است. در همین راستا رتبه ایران در این بخش ۶۷ است. اما در حوزه سرعت دانلود با پهنای باند ثابت ایران با سرعت دانلود ۱۰.۲۸ مگابایت بر ثانیه و آپلود **Mbps ۴.۹۲** در رتبه ۱۰۵ قرار دارد. این در حالی است که نروژ با سرعت دانلود موبایل ۶۲.۶۶ مگابایت بر ثانیه در رتبه اول این فهرست قرار دارد. پس از آن هلند با سرعت **Mbps ۵۳,۰۱**، ایسلند با **Mbps ۵۲,۷۸** در ثانیه قرار گرفته‌اند. در شاخص سرعت دانلود با پهنای باند ثابت نیز کشور سنگاپور با سرعت ۱۵۳.۸۵ مگابایت بر ثانیه در رتبه نخست قرار دارد. پس از آن ایسلند با سرعت **Mbps ۱۴۷,۵۱** و هنگ کنگ با سرعت **Mbps ۱۳۳,۹۴** قرار دارند. در هر حال ماه نوامبر **Speedtest** اعلام کرد سرعت دانلود موبایل در ۱۱۹ کشور بیش از متوسط جهانی ۲۰.۲۸ مگابایت بر ثانیه است. همچنین در ۱۳۴ کشور این شاخص کمتر از متوسط جهانی است. پهنای باند در ۷۱ کشور بالاتر از متوسط جهانی و ۱۸۵ کشور کمتر از این شاخص است. همچنین کشورهای لائوس، ویتنام، ترینیداد، هنگ کنگ و لبنان شاهد بیشترین افزایش سرعت اینترنت موبایل بودند.