

خبر

روزهای دشوار مایکروسافت در رقابت با اپل



انتظار می‌رود مایکروسافت بعد از ۲۰ سال، سود کمتری در مقایسه با اپل در میان

شرکت‌های فناوری کسب‌کنند.

به گزارش اپل‌اینسایدر، در حالی که بازار رایانه‌های شخصی در حال نزول است، بازار گوشی و تبلت و نوت‌بوک روز به روز پیشرفت بیشتری می‌کند و همین مساله موجب شده اپل با تولیدات خود گوی سبقت را از مایکروسافت برپایند. پیش‌بینی‌ها حاکی است اپل در سه‌ماهه اول سال ۲۰۱۱ بیش از شش میلیارد دلار درآمد داشته باشد که این رقم بیشتر از درآمد پیش‌بینی شده مایکروسافت طی این مدت یعنی ۵/۹۳ میلیارد دلار است. نکته جالب اینکه تنها دو سال قبل درآمد سه‌ماهه اول مایکروسافت دو برابر اپل بود. اما وضعیت اپل در دو سال اخیر دگرگون شده و این شرکت بازارهای جدیدی را در حوزه گوشی‌های هوشمند و رایانه‌های لوحی به وجود آورده و بسیاری از رقبا را پشت سر گذاشته است. اگرچه هنوز سالانه بیش از ۳۰۰ میلیون رایانه که بر روی آنها سیستم عامل ویندوز نصب شده، به فروش می‌رود، اما مایکروسافت نتوانسته هم‌پای تحولات جلو برود و بازار گوشی‌های هوشمند و تبلت را از دست داده است. ویندوز فون ۷ سیستم عامل مایکروسافت برای گوشی‌ها هم چندان موفق نبوده و با این حساب روزهای دشواری برای این شرکت پیش روی ماست.

گیگابایت به جر که تبلت‌سازان بیوست



شرکت گیگابایت نخستین تبلت خود را تولید و معرفی کرد. به گزارش ایثنا این محصول که S1080 نام دارد از یک صفحه ۱۰/۱ اینچی با قابلیت مولتی‌تچ بهره می‌برد. سیستم عامل به کار رفته در این تبلت Windows 7 است و توان پردازشی آن توسط یک پردازنده Intel Atom N550 دو هسته‌ای تامین می‌شود. به همین دلیل S1080 از تمامی نرم‌افزارها و قابلیت‌های ویندوز پشتیبانی کرده و کاربران می‌توانند تمامی نیازهای مربوط به ایمیل و اینترنت و آفیس خود را توسط آن برطرف کنند. این تبلت کمتر از یک کیلوگرم، تقریباً ۹۰۰ گرم وزن داشته و از این رو به راحتی قابل حمل است. در ضمن یک هارددیسک ۳۲۰ گیگابایتی در این تبلت قرار گرفته است که کاربران را از حمل هارددیسک‌های اکسترنال بی‌نیاز می‌کند. از دیگر قابلیت‌های کاربردی و منحصر به فرد این تبلت می‌توان به داشتن درگاه USB3, 0 اشاره کرد که برای انتقال بسیار سریع اطلاعات بهترین گزینه است. صفحه نمایش این تبلت مجهز به نور پس‌زمینه TFT-LCD با وضوح ۱۰۲۴ در ۶۰۰ است و تصاویر را با شفافیت بالایی به نمایش درمی‌آورد. در ضمن یک خروجی گرافیکی نیز روی این تبلت تعبیه شده است تا بتوان تصاویر را به یک صفحه نمایش خارجی یا ویدئوپروژکتور منتقل کرد. این تبلت برای اتصال به اینترنت از Wi-Fi 802.11b/g/n بهره می‌برد و به واسطه دوربین ۱/۳ مگاپیکسلی آن، می‌توانید به راحتی با دوستان خود ارتباط تصویری برقرار کنید.

گوگل شش هزار کارمند جدید استخدام می‌کند

گوگل درصدد است تا پایان سال جاری میلادی شش هزار و ۲۰۰ کارمند جدید

استخدام کند.

به گزارش ایسنا پس از اینکه رئیس‌جمهور آمریکا در سخنرانی خود برای مقامات تجاری و اقتصادی آمریکا خواستار اشتغال‌زایی بیشتر شد، مدیر اجرایی گوگل اعلام کرد تا پایان سال ۲۰۱۱ نزدیک به شش هزار و ۲۰۰ کارمند جدید به استخدام این شرکت درخواهند آمد. گوگل در سال ۲۰۱۰ نیز شاهد افزایش نیروی ۲۳ درصدی بود. به گفته مدیر اجرایی گوگل، در سال ۲۰۱۱ مهندسان باهوش رایانه و نمایندگان فروش بیشتری به جمع کارمندان گوگل اضافه خواهند شد تا برتری این شرکت در بازار جست‌وجوی اینترنتی و تبلیغات حفظ شود. پیش از این گوگل در سال ۲۰۰۷ نیز شش هزار و ۱۳۱ کارمند جدید استخدام کرده بود و در سال ۲۰۱۰ نیز چهار هزار و ۶۰۰ کارمند جدید به گوگل ملحق شدند و در پایان سال ۲۰۱۰ شمار مجموع کارکنان گوگل ۲۴ هزار و ۴۰۰ نفر بود.

اخراج ۱۵۰ کارمند یاهو

یاهو اعلام کرد نزدیک به ۱۰۰ تا ۱۵۰ کارمند خود را به‌زودی اخراج خواهد کرد.

به گزارش ایسنا به دنبال افزایش فشارهای مالی بر یاهو به خاطر کاهش عرضه سهام این شرکت در بازار بورس،مقامات یاهواعلام کردندبه‌زودی ۱۰۰ تا ۱۵۰ کارمند کشور اخراج خواهند شد.یاهو در صورت اخراج این تعداد از کارمندان،شاهد کاهش یک‌درصدی در شمار کارمندان خود خواهد‌بود.اخیراً ارزش سهام یاهو در بازار بورس کاهش یافته و همین‌اثر باعث شده‌مقامات این شرکت به‌فکر راهکارهایی جهت حفظ درآمدهای خود باشند.

بنا بر اظهارات عضو رسیدگی به جرائم رایانه‌ای و دعاوی اینترنتی دادگستری کل تهران ثبت مشخصات کاربران در کافی‌نت‌ها مغایر با حقوق شهروندی بوده و دستورالعمل واحدی برای این اقدام از سوی قوه قضائیه صادر نشده است. این رئیس کل دادگستری استان آذربایجان شرقی اعلام کرد از این پس متصدیان کافی‌نت‌ها ملزم هستند مشخصات کاربران خود را با درج کد ملی و زمان استفاده از رایانه ثبت کنند. او که در جلسه ستاد پیشگیری و مبارزه با جرائم خاص استان آذربایجان شرقی سخن می‌گفت، بیان کرد بیشتر تخلفات و جرائم رایانه‌ای در کافی‌نت‌ها صورت می‌گیرد که درج مشخصات کاربران می‌تواند تا حد زیادی از وقوع جرم جلوگیری کند. در عین حال مدیران برخی کافی‌نت‌ها نیز بیان می‌کنند در حال حاضر دستورالعملی از سوی قوه قضائیه برای آنها ارسال نشده اما با این وجود هر از چند گاهی

ماموران نیروی انتظامی برای بازدید از برخی کافی‌نت‌ها مراجعه کرده و در مورد کاربران پرسش‌هایی را مطرح می‌کنند. از طرفی هر چند مقام مسئول در دادگستری استان آذربایجان بر این باور است که بیشتر تخلفات و جرائم رایانه‌ای در کافی‌نت‌ها صورت می‌گیرد اما به گفته بهرام سپهری مدیر کافی‌نت وجود فیلترینگ در کافی‌نت‌ها از بروز بسیاری تخلفات جلوگیری می‌کند. از طرفی اداره امکان نیز به ما اجازه نرم‌افزارهای فیلترینگ را نمی‌دهد. شامین بهرامی مسوول یکی از کافی‌نت‌ها نیز بیان می‌کند بیشترین دقت مسوولان کافی‌نت‌ها بر مسائلی مانند سرقت و هک در کافی‌نت‌هاست که مبدا روی دهد. مداه‌ای به صورت مجزا در قانون در مورد کافی‌نت‌ها وجود ندارد، اما اعضای این صنف موظفند بر اساس مصوباتی که هنگام صدور مجوز در اتحادیه و آیین‌نامه‌ای که در سازمان تنظیم مقررات و ارتباطات رادیویی به امضا می‌رسانند، نحوه عملکرد خود را تنظیم کنند. نکته قابل توجه این است که بسیاری از اتحادیه‌ها در استان‌ها نسبت به اجرای برخی قوانین صدور مجوز و نظارت بر فعالیت کافی‌نت‌ها پیشدستی کرده و می‌توان گفت مسیر را برای بروز جرائم رایانه‌ای مسدود کرده است. برای نمونه اتحادیه کامپیوتر مشهد در تازه‌ترین دستورالعمل خود برای این منظور آورده است ارائه خدمات به کاربران بدون ارائه مدارک هویتی معتبر ممنوع است. متصدی مکلف است پس از رویت اصل مدارک هویتی معتبر و تطبیق عکس، نام و نام خانوادگی، نام پدر، شماره شناسنامه، محل صدور و کد ملی را دقیقاً ثبت کند. البته این دستورالعمل به صورت سراسری بوده و تمامی اتحادیه‌های استانی آن را برای کافی‌نت‌های خود ارسال کرده‌اند؛ دستورالعملی ۱۵ ماده‌ای که بسیاری از مسوولان کافی‌نت‌ها وجود برخی از بندهای آن را غیرقابل اجرا می‌دانند.

مقاوت ثبت مشخصات با حفظ حریم خصوصی
بنا بر اظهارات عضو کمیته حل اختلاف جرائم رایانه‌ای ثبت مشخصات کاربران اینترنت با حفظ حریم خصوصی افراد مغایرت دارد و تنها در مواردی خاص که قاضی پرونده احتیاج به رهگیری یک IP ادرس داشته باشد، طبق قانونی می‌تواند از مخابرات با کافی‌نت‌های مورد را پیگیری کند. به گفته یاقار افخمی اگر دستورالعملی مبنی بر ثبت مشخصات کاربران در کافی‌نت‌ها از سوی قوه قضائیه به ثبت شود به صورت متمرکز خواهد بود که در این صورت باید یک تفاهنامه کاری از سوی قوه قضائیه و وزارت ارتباطات منعقد شود چراکه این موضوع تنها مربوط به مجتمه‌های اساسی، آیین‌نامه

بنا بر اظهارات عضو کمیته حل اختلاف جرائم رایانه‌ای ثبت مشخصات کاربران اینترنت با حفظ حریم خصوصی افراد مغایرت دارد و تنها در مواردی خاص که قاضی پرونده احتیاج به رهگیری یک IP ادرس داشته باشد، طبق قانونی می‌تواند از مخابرات با کافی‌نت‌های مورد را پیگیری کند. به گفته یاقار افخمی اگر دستورالعملی مبنی بر ثبت مشخصات کاربران در کافی‌نت‌ها از سوی قوه قضائیه به ثبت شود به صورت متمرکز خواهد بود که در این صورت باید یک تفاهنامه کاری از سوی قوه قضائیه و وزارت ارتباطات منعقد شود چراکه این موضوع تنها مربوط به مجتمه‌های اساسی، آیین‌نامه

گذرگاه قانون

اعلام شرایط جدید فعالیت کافی نت‌ها

نشستن زن و مرد حتی محارم کنار یکدیگر ممنوع شد

حامد شفیعی



- متن کامل شرایط جدید کافی‌نت‌ها**
- ۱- متقاضی باید دارای حداقل ۳۰ سال سن و متاهل باشد.
- ۲- دارا بودن گواهی پایان دوره ICDL از مراکز معتبر یا تحصیلات مرتبط با رایانه، شبکه و اینترنت یا تایید کمیسیون فنی اتحادیه.
- ۳- نصب دوربین مداربسته (مشخصات فنی دوربین توسط اتحادیه پس از اخذ تاییدیه از کمیته تخصصی تعیین خواهد شد)
- ۴- واحد صنفی باید در حاشیه خیابان باشد.
- ۵- واحد صنفی داخل پاساژ نباشد.
- ۶- واحد صنفی داخل طبقه نباشد.
- ۷- واحد صنفی نزدیک مراکز آموزشی دخترانه نباشد.
- ۸- واحد صنفی کاملاً آکواریم و دارای شیشه بی‌رنگ باشد به طوری که داخل واحد صنفی از بیرون کاملاً قابل رویت باشد.
- ۹- چسباندن هر نوع پوستر یا کشیدن پرده یا حصیر که باعث شود داخل مغازه از بیرون قابل رویت نباشد ممنوع است.
- ۱۰- نشستن زن و مرد حتی محارم کنار یکدیگر ممنوع است.
- ۱۱- از گذاشتن نام خارجی و اصطلاحات بیگانه جهت واحد صنفی جداً خودداری کنید. جهت انتخاب نام با دبیرخانه هماهنگی کنید.
- ۱۲- داشتن کیسول ضدحریق و جعبه کمک‌های اولیه الزامی است.
- ۱۳- ساعت ورود و خروج مراجعان باید در دفتر مخصوصی ثبت شود.
- ۱۴- ارائه خدمات به کاربران بدون ارائه مدارک هویتی معتبر ممنوع است. متصدی مکلف است پس از رویت اصل مدارک هویتی معتبر و تطبیق عکس، نام و نام‌خانوادگی، نام پدر، شماره شناسنامه، محل صدور و کد ملی را دقیقاً ثبت کند.
- ۱۵- متصدی مکلف به نگهداری اطلاعات مندرج در بند ۱۴ به مدت شش ماه و نگهداری اطلاعات دوربین مداربسته به مدت سه ماه است. در غیر این صورت مسوولیت قانونی خواهد داشت.

قضایی و کافی‌نت‌ها نبوده و به وزارت ارتباطات نیز مربوط می‌شود. با این حال شریفی رئیس دادگستری استان آذربایجان شرقی با بیان آمارهایی از وضعیت کافی‌نت‌ها در تبریز بیان می‌کند متأسفانه از ۲۵۰ کافی‌نت موجود در تبریز فقط ۹۸ کافی‌نت مجوز فعالیت دارند که کافی‌نت‌های غیرمجاز در اسرع وقت تعطیل شده و در صورت دریافت مجوز اجازه فعالیت داده خواهد شد.

رئیس کل دادگستری استان همچنین شرکت مخابرات استان را مکلف به تشکیل کمیته‌ای نظارتی کرد و خواست این شرکت از ارائه خدمات به کافی‌نت‌های غیرمجاز خودداری کند. هرچند این مقام مسوول قضایی راهکارهایی را برای پیشگیری از جرائم رایانه‌ای مطرح می‌کند اما او همچنین نظارت بر کافی‌نت‌ها و اعطای مجوز در صورت احراز شرایط را مهم‌ترین مولفه در این زمینه می‌داند.
این حال کارشناسان ثبت اطلاعات افراد در کافی‌نت‌ها را مغایر با قانون اساسی می‌دانند. به گفته آنها حریم خصوصی افراد در ایران مصون دانسته شده و هیچ کس حق ورود

گذرگاه قانون

آیین‌نامه نحوه اجرای فعالیت‌های مشخص برای توسعه‌فاوا

اجرای کشور به ویژه دستگاه‌هایی که به طور مشخص برنامه‌های طرح توسعه کاربری فناوری اطلاعات و ارتباطات مورد خطاب آنهاست، مکلفند به صورت همه‌جانبه و با اولویت ویژه نسبت به تجهیز و

بسیج امکانات خود برای محقق شدن دستوردهای طرح اقدام کنند. نکته قابل تأمل دیگر در این مصوبه تأکید بر حضور بخش خصوصی به عنوان محور کلیدی است چرا که بر اساس این مصوبه به منظور جلوگیری از توسعه تصدی دولتی و همچنین بسط فرصت‌ها و انگیزه‌های لازم برای تحرک بخشیدن به فعالیت بخش خصوصی به عنوان محور کلیدی و راهبردی حرکت توسعه فناوری اطلاعات و ارتباطات در کشور، در اجرای مواد ۲ و ۳ و تبصره ۲ ماده ۴ قانون برنامه سوم توسعه اقتصادی، اجتماعی و فرهنگی ایران، خرید خدمات یا انعقاد قرارداد مربوط به طرح‌ها و پروژه‌های فناوری اطلاعات و ارتباطات با دستگاه‌ها و شرکت‌های دولتی مستلزم جذب موافقت سازمان مدیریت و برنامه‌ریزی کشور است. عین حال گزارش‌های تکمیلی باید هر سه ماه یک بار به رئیس‌جمهوری و معاون اول وی تقدیم شود تا در صورت لزوم در دستور کار هیات دولت قرار گیرد.
نکته آخر اینکه وزارت ارتباطات و فناوری اطلاعات و شرکت‌های مخابراتی ایران و استان‌ها مکلفند نسبت به سرمایه‌گذاری لازم برای توسعه شبکه دیتای کشور مطابق با نیازهای طرح جامع توسعه و کاربرد فناوری اطلاعات و ارتباطات اقدام کنند.

نخواهد بود.
افخمی در این باره ادامه می‌دهد قانون هر کشور تابع شرایط سرزمینی است و چنانچه الزامی برای ثبت مشخصات کاربران

اطلاع عموم برسد و به عنوان یک دستورالعمل ابلاغ شود. اما به نظر می‌رسد تنها برای شهرهای شیراز، اصفهان، تبریز و مشهد شرایط و قوانین جدید بر کافی‌نت‌ها اعلام شده است، شرایط پانزده گانه‌ای که طیفی به گستردگی مسائل شرعی چون ممنوعیت نشستن حتی محارم کنار یکدیگر تا مسائل امنیتی شامل ارائه خدمات تنها به شرط ثبت مشخصات کامل مراجعه‌کننده و حفظ آن را دربردارد. مساله قابل توجه در این شروط تغییر ساعت کاربری آقایان با خاتمه‌است که در صورت تغییر ساعات کاربری آقایان با خانم‌ها به با متخلفان کافی‌نت‌ها برخورد خواهد شد. با این حال مسوولان کافی‌نت‌ها با طرح پرسش‌هایی در این زمینه بیان می‌کنند سوال اینجاست که آیا متصدی کافی‌نت می‌تواند واقعاً این قوانین را در محل کار خود اجرا کرده و به ثبت مشخصات شناسنامه‌ای و کد ملی مراجعان و مانع شدن از نشستن محارم در کنار یکدیگر بپردازد؟ آیا امکان این هست که زن و شوهری دیگر برای ثبت‌نام عتبات‌عالیات پشت کامپیوتر نشسته‌اند یا پدر و دختری را که در حال انتخاب واحد و پرداخت الکترونیک شهریه دانشگاه هستند به دو قسمت مجزای کافی‌نت هدایت کرد؟ به گفته سپهری یکی از مسوولان کافی‌نت‌ها شاید در گوشه و کنار شهر افرادی بدون مجوز و غیرمسوول در بسیار پسندیده است با این‌گونه افراد برخورد جدی شود و حتی در صورت داشتن پروانه کسب اتحادیه می‌تواند پروانه فرد خاطی را باطل کند. اما مسلط دادن این گونه جرائم به کلیه کافی‌نت‌ها و به جای نظارت دقیق و برخورد قاطع، صدور چنین بخشنامه‌هایی که نمی‌توان اجرا کرد که جای تامل بیشتری دارد؟ او ادامه می‌دهد: «جا دارد اتحادیه‌ها به جای ابلاغ این گونه قوانین با نظارت بیشتر جلوی ارتکاب جرم را بگیرند و قدیمی نیز در حمایت از اعضای تحت پوشش و رفع مشکلات بی‌شمار این صنف از قبیل پیگیری قطعی‌های مکرر اینترنت و برخورد با تداخل شغلی سایر اصناف که خدمات اینترنتی می‌دهند و ده‌ها مشکل دیگر بر دارند نه اینکه فقط و فقط سالانه مبلغی به عنوان حق‌ضویت‌ترقی‌تکند»

بهرامی یکی دیگر از مسوولان کافی‌نت‌ها نظرات خود را با پرسش‌هایی در این زمینه مطرح می‌کند که آیا با نظارت دستگاه‌های موازی متعدد نظیر بازرسی اتحادیه، مجمع امور صنفی، بازرسی اداره بازرگانی، اداره نظارت بر اماکن عمومی و حتی پاسگاه انتظامی محل بر کار کافی‌نت‌ها باز هم در این صنف تخلف صورت می‌گیرد؟ و اگر صورت می‌پذیرد آیا مشکل از نظارت دستگاه‌های فوق نیست؟ با این حال مباحث مربوط به حریم خصوصی در چهار حوزه شامل «حریم خصوصی جسمانی»، «حریم خصوصی در منازل و اماکن»، «حریم خصوصی اطلاعاتی» و «حریم خصوصی ارتباطاتی» قابل تقسیم هستند. یکی از مباحث مهم مربوط به حریم خصوصی افراد، مصون بودن داده‌های مربوط به حوزه زندگی انسان‌هاست، که با حفظ صحت اطلاعات و محرمانگی آنها محقق می‌شود. اصل ۲۵ قانون اساسی نیز هرگونه تجسس را ممنوع دانسته است که در تفقح حریم خصوصی افراد، در بسیاری از موارد مفهوم تجسس احراز می‌شود.

بنا بر اظهارات عضو اصلی مجتمع رسیدگی به جرائم رایانه‌ای و دعاوی اینترنتی دادگستری کل استان تهران طبق اعلام ریاست قوه قضائیه، قضات برای رسیدگی به پرونده‌ها حق ورود به حریم خصوصی افراد را ندارند. از طرفی ثبت کد ملی کاربران در کافی‌نت نمی‌تواند مبنای دقیقی برای رهگیری اطلاعات باشد چرا که پیگیری پرونده‌های مرتبط با جرائم رایانه‌ای از طریق IP ادرس‌ها انجام می‌شود و اینکه چه شخصی و در چه ساعتی از کامپیوتر استفاده کرده مبنای دقیقی

دنیای نرم‌افزار

تبدیل متن به گفتار به کمک نرم‌افزار

در زمینه تبدیل متن به گفتار است، یعنی این نرم‌افزار قادر است متنی را برای کاربر بخواند. به عنوان مثال شما قصد دارید به یک سایت خبری که هر روز به مطلب آن توجه می‌کنید و جای روزنامه را برای شما

گرفته است هنگام انجام کاری دیگر گوش دهید.

است متن مورد نظر را به برنامه داده و اقدام به تبدیل متن به گفتار کنید. حال قادرید مطلب مورد نظر را به جای خواندن گوش کرده و به امور دیگر خود نیز بپردازید. این نرم‌افزار دارای ویژگی‌های بسیاری است که از جمله آن می‌توان به این موارد اشاره داشت:
قابلیت تبدیل متن به گفتار و ذخیره‌سازی آن در فرمت‌های MP3 و Wav، پشتیبانی از چند زبان مختلف، قابلیت تبدیل سریع متن به فایل صوتی، پشتیبانی از فونت‌های مختلف متنی و دارای تنظیمات فونت و ده‌ها ویژگی برتر دیگر.

به هر حال اگر شما علاقه‌مند هستید که این نرم‌افزار قوی را روی سیستم خود بارگذاری کنید و به اطلاعات جامعی در خصوص آن دست پیدا کنید به شما توصیه می‌کنیم حتماً سری به سایت p30world.com بزنید تا علاوه بر کسب اطلاعات به طور رایگان این نرم‌افزار را تهیه کنید.

گفتنی است این نرم‌افزار قوی محصولی از شرکت Zero2000 Software است. به شمار می‌آید که مخاطبان بسیاری در سراسر جهان دارد.

سال پنجم ■ شماره ۱۱۷۲ **شرق** *روزانه*

ترفند

ایمن‌سازی در مقابل خطرات مدرن وب

آموزش و آگاهی دادن به کاربران، راهکارهای پیشگیرانه و استفاده از راه‌حل‌های امنیتی مدرن وب، از اجزای یک دفاع همه‌جانبه در برابر تهدیدات جدید به شمار می‌روند. به گزارش ایسنا، چندین روش پیشگیرانه و ضروری وجود دارد که پیاده‌سازی آنها به کاهش خطرات منجر شده و تا حد امکان کاربر را از تهدیدات اینترنتی جدید دور نگه می‌دارند. در این مطلب شما را با نکاتی در این خصوص آشنا می‌کنیم.

به‌روزرسانی سیستم را جدی بگیرید

سیستم عامل، مرورگر، plug-inهای مرورگرها، media players PDF Reader و دیگر برنامه‌های کاربردی باید به‌روزرسانی شوند. این کار می‌تواند خسته‌کننده و وقت‌گیر باشد اما متأسفانه هکرها نیز روی افرادی حساب می‌کنند که اطلاعات یا حوصله کافی را برای به روز نگه داشتن سیستم‌های خود ندارند. بسیاری از بدافزارهای وب، از کدهای سوءاستفاده آماده‌ای استفاده می‌کنند که به صورت تجاری در دسترس بوده و حاوی ده‌ها تست‌کننده آسیب‌پذیری مختلف، redirectorها و کدهای سوءاستفاده واقعی هستند. اغلب این کدهای سوءاستفاده‌کننده به محض شناسایی هر نقض امنیتی به آن حمله می‌کنند. این بسته‌های بدافزار برای سوءاستفاده از افرادی ساخته شده است که آگاهی کافی برای به‌روزرسانی و نصب اصلاحیه‌های نرم‌افزارها و سیستم عامل رایانه خویش را ندارند. اهداف اصلی این بسته‌های بدافزار مبتنی بر وب نه‌تنها شامل سیستم عامل و مرورگرهای وب همچون IE، فایرفاکس Safari Chrome و Opera می‌شود بلکه plug-in های مشترک بین مرورگرها همچون PDF Reader، Flash Player، Quick Time و محیط اجرایی جاوا را نیز در برمی‌گیرد.

استفاده از نرم‌افزارهای وب استاندارد فراموش نشود

در صورتی که نکته‌شماره ۱ را مطالعه کرده باشید، ممکن است هنوز هم فکر کنید نگهداری سیستم در وضعیت کاملاً به‌روز، در حالی که تمام اصلاحیه‌های امنیتی نیز روی آن نصب شده‌اند، کار بسیار طاقت‌فرسایی است. اما موضوع زمانی پیچیده‌تر می‌شود که ندانید چه نرم‌افزارهایی روی شبکه شما اجرا می‌شوند یا کاربران شبکه از مرورگرها، Pluginها و Media Playerهای مختلف و متفاوتی استفاده کنند. در این صورت است که کار به‌روزرسانی دائمی نرم‌افزارها بسیار سخت و تقریباً غیرممکن می‌شود. همان‌طور که قبلاً گفته شد، حملات مدرن و به‌معمولاً با استفاده از بسته‌های بدافزاری آماده که برای سوءاستفاده از صدها آسیب‌پذیری در نرم‌افزارهای مختلف طراحی شده‌اند، انجام می‌شوند. بنابراین گستردگی بیشتر دامنه سکو‌ها و نرم‌افزارهای مورد استفاده در شبکه، فرصت بیشتری را برای سوءاستفاده از سیستم‌های موجود در شبکه در اختیار هکرها قرار می‌دهد. همچنین احتمال کشف یک آسیب‌پذیری در یک برنامه کاربردی که اصلاحیه آن به موقع نصب نشده است، افزایش می‌یابد. بهترین کار برای کاهش چشمگیر سطح تهدیدات، ایجاد یک مجموعه کوچک از برنامه‌های کاربردی اساسی برای ارتباط با اینترنت و ملزم کردن کاربران به استفاده از آنهاست.

ایمن‌سازی مرورگرها

شما باید با امکانات مختلف امنیتی مرورگرتان آشنایی پیدا کنید زیرا برخی از تنظیمات امنیتی ثبت تعداد هشدارها را افزایش می‌دهند و بدون اینکه تأثیر خاصی روی سطح امنیتی داشته باشند، تنها باعث آذیت و آزار کاربر می‌شوند، در حالی که برخی تنظیمات دیگر اهمیت بسزایی در کاهش سوءاستفاده‌ها و تهدیدات دارند.

استفاده از کلمه عبور قدرتمند

هدف از سیاست اعلام کلمه عبور بسیار واضح است: در صورتی که نمی‌خواهید هر کسی به فایل یا اطلاعات مشخصی دسترسی داشته باشد، یک کلمه عبور را تعیین می‌کنید تا تنها افراد مجاز قادر به دسترسی به اطلاعات مذکور باشند. هدف از ایجاد یک کلمه عبور موثر، حفظ کلمات عبور از به آسانی حدس زده شدن یا شکسته شدن توسط هکرهاست. علاوه بر تعداد زیاد آسیب‌پذیری‌های موجود در سیستم‌ها، برخی سازمان‌ها حتی این راهکار موثر و ساده کاهش خطر را نیز رعایت نمی‌کنند.

امنیت وب را جدی بگیرید

یک راهکار امنیت وب مناسب، یکی از اجزای ضروری استراتژی یکی برای محافظت از سازمان در برابر تهدیدات مدرن وب است. یک راه‌حل امنیتی مناسب، با محدود کردن مجموعه کاربران به وب‌سایت‌هایی که مرتبط با کار آنهاست (یا حداقل ممناعت از دسترسی آنها به وب‌سایت‌های غیرمجاز و آلوده که زمینه مناسبی برای رشد بدافزارهاست)، خطرات را کاهش می‌دهد. این راه‌حل همچنین از شما در برابر وب‌سایت‌های قانونی و مطمئنی که هر روز به آنها مراجعه می‌کنید، اما ممکن است در دست هکرها افتاده باشند تا بی‌سرو صدا به انتشار بدافزار بپردازند، محافظت به عمل می‌آورد. بالاخره چنین راه‌حلی به حفظ منابع اینترنت در برابر سوءاستفاده‌هایی همچون انتقال اطلاعات غیرمجاز یا سرقت پهنایی باند کمک می‌کند. فیلتر کردن بر اساس کارایی و شهرت وب‌سایت‌ها یک سیاست کاربری قابل قبول را ارائه می‌دهد و همچنین از گسترده شدن تهدیدات وب‌سایت‌های بندانم و خرابکار جلوگیری به عمل می‌آورد. از طرف دیگر این سیاست، وب‌سایت‌های با شهرت بد را نیز مستقل از طبقه‌بندی آنها فیلتر می‌کند. فیلتر کردن پراکسی به کاربران اجازه نمی‌دهد از محدودیت‌های اعمال‌شده در فیلتر گذر کرده و در نتیجه خود و سازمان مربوطه را به خطر اندازند. فیلتر کردن بلادرنگ بدافزارها، آنها را بلافاصله در زمان دریافت از یک وب‌سایت خرابکار گیر می‌اندازد. همچنین فیلتر کردن بر اساس محتوا، از طرفی انواع فایلی را که معمولاً با بدافزارها همراه هستند شناسایی می‌کند و از طرف دیگر چگونگی مصرف پهنای باند را زیر نظر دارد. با رعایت همه نکات مذکور می‌توانید تا حد بسیار زیادی از بروز حملات در شبکه جلوگیری به عمل آورید و امنیت شبکه را به سطح مطلوب و قابل قبولی برسانید.