دنیای
کامپیوتر و ارتباطات

بخش ویژه

برخی عناوین این بخش:

- ۱۰ مدیر برتر امنیتی خاورمیانه
- مکانی برای تلاقی امنیت و رایانه
- تهدیدات امروز، ابزار به‌روز
- ضامن امنیت مکاتبات شما
- پاسخگویی به تمام نیازهای امنیتی
- رونمایی از راهکار ایده‌آل کسپرسکی برای سازمان‌ها

حملات سایبری دولت چین به آمریکا تایید شد

به دنبال هک شدن مراکز رسانه‌ای آمریکایی از جمله New York Times، Washington Post و Wall Street Journal طی هفته‌های گذشته و همچنین شرکت‌های تجاری بزرگ و کوچک آمریکا طی یک سال قبل، احتمال می‌رفت که این حملات از داخل کشور چین هدایت شوند. اما هم‌اکنون با انجام بررسی‌های مختلف در این زمینه تایید شد که تمامی این حملات را چین پشتیبانی می‌کرده است.

به گزارش ایتنا روزنامه نیویورک تایمز در گزارشی توضیح داده است که شرکت امنیتی آمریکایی Mandiant به زودی گزارشی ۶۰ صفحه‌ای منتشر می‌کند که جزئیات بین گروه‌های هکری چینی و همچنین دولت چین در آن آورده شده است و نشان می‌دهد که دولت چین در اقدامات امنیت سایبری اخیر علیه آمریکا دست داشته است. بر اساس این گزارش گفته شده است که عملیات‌های اخیر از داخل ساختمانی در نزدیکی شهر شانگهای که دفتر مرکزی "ارتش آزادی‌بخش چین" در آن واقع شده، صورت گرفته است.

دولت چین همچنان این اتهامات وارده را

تکذیب می‌کند، اما کوین ماندیا موسس شرکت امنیتی Mandiant توضیح داده است که مستندات فراوانی برای حملات سایبری دولت چین وجود دارد. منابع آگاه گزارش داده‌اند که بسیاری از آژانس‌های امنیتی و سازمان امنیت اطلاعات آمریکا هم‌اکنون به این یقین رسیده‌اند که حملات سایبری و تخریب‌های اینترنتی اخیر در این کشور توسط گروه‌های هکری چینی صورت گرفته است که مرکز آنها واحد ۶۱۳۹۸ در ساختمان مرکزی "ارتش آزادی‌بخش چین" بوده است. ❖

صنعت خرده فروشی؛ مهم‌ترین هدف مجرمان سایبری در سال ۲۰۱۲

نتایج مطالعه یک شرکت پژوهشی نشان داده است صنعت خرده فروشی در سال ۲۰۱۲ در راس اهداف مجرمان سایبری بوده است. به گزارش ایتنا از همکاران سیستم به نقل از وب سایت zdnet، نتایج پژوهش‌های شرکت Trustwave نشان می‌دهد در سال ۲۰۱۲ حدود ۴۵ درصد از حملات سایبری متوجه صنعت خرده فروشی بوده است که این میزان حدود ۱۵ درصد از سال قبل بیشتر است.

یافته‌های این مطالعه نشان می‌دهد که در این سال سهم حملات صنایع مواد غذایی و نوشیدنی، بیمارستان‌ها و صنعت خدمات بهداشتی و صنعت خدمات مالی به ترتیب ۲۴، ۹ و ۷ درصد این حملات بوده است. در این میان سازمان‌های غیرانتفاعی کمتر از دیگر سازمان‌ها و شرکت‌های دیگر مورد هدف حمله مجرمان سایبری قرار گرفته‌اند. در سال ۲۰۱۲ سهم این سازمان‌ها از این حملات فقط ۳ درصد بوده است.

به گفته تحلیلگران صنعت خرده فروشی به این دلیل بیش از سایر صنایع هدف حمله بدافزارها قرار گرفته که مشتریان زیادی با آن سر و کار دارند و حجم وسیعی از پرداخت‌های کارتی و اعتباری نیز از طریق این صنعت انجام می‌شود.

یافته‌های شرکت تراست ویو نیز نشان می‌دهد ۹۶ درصد از اطلاعاتی که توسط مجرمان سایبری هدف قرار گرفته، متعلق به کد داده‌هایی مثل اطلاعات مربوط به کارت‌های اعتباری، اطلاعات کارت‌های شناسایی و آدرس ایمیل مشتریان است. شرکت تراست ویو همچنین دریافته است که کسب و کارهای تجاری در سال گذشته در شناسایی فعالیت‌های مشکوک و مجرمانه کندتر از سال‌های قبل عمل کرده‌اند. یافته‌های مطالعات مشابهی که در سال‌های قبل انجام گرفته نشان می‌داده که به طور متوسط کسب و کارها ۱۷۵ روز بعد از حمله متوجه فعالیت‌های مشکوک در عملیات خود شده‌اند. این زمان در سال ۲۰۱۲ با ۳۵ روز افزایش به ۲۱۰ روز رسیده است. ❖

هشدار به شرکت‌ها: برای تامین امنیت خسّت به خرج ندهید

شرکت‌هایی که بخش اعظم بودجه امنیتی خود را صرف امور حاشیه‌ای می‌کنند، به طور قطع هدف سرقت‌های بزرگ سایبری قرار می‌گیرند. به گزارش ایتنا از فارس به نقل از وی تری، گروهی از مدیران برجسته چند موسسه امنیتی معتقدند شرکت های تجاری باید پول بیشتری برای حفظ امنیت خود در فضای مجازی هزینه کنند و مراقب وضعیت شبکه‌های رایانه‌ای خود هم باشند. برخی شرکت‌ها که تصور درستی در مورد نحوه حفظ امنیت خود ندارند، صرفاً بر روی خرید فایروال و نرم‌افزارهای سنتی ضدویروس متمرکز می‌شوند و در عمل نمی‌توانند از داده‌های شخصی خود بر روی وب و در داخل شبکه‌های محلی به خوبی محافظت کنند. با توجه به تحول در شیوه‌های نفوذ به رایانه‌ها و استفاده گسترده هکرها از انواع بدافزارهای تحت شبکه که توسط ضدویروس‌های سنتی قابل تشخیص و نابودسازی نیستند، ضروری است شرکت‌های تجاری در رویگرد خود به امنیت تجدیدنظر کنند. به اعتقاد شرکت‌های ArcSight، DVLabs و Fortify آنها باید با درک ویژگی‌های محیط وب و تهدیدات آن برای مقابله با خطرات فزاینده موجود برنامه‌ریزی کنند. در کنار مقابله با تهدیدات اینترنتی، شناخت تهدیدات داخلی و محلی و آموزش به کارکنان در این زمینه هم اهمیت دارد، زیرا در بسیاری از موارد کارکنان به علت بی‌اطلاعی و با باز کردن یک ضمیمه ایمیل آلوده خسارات سنگینی به شرکت محل کار خود وارد می‌کنند. ❖

با فرمان اوباما سیاست اجرایی امنیت سایبر تهیه می‌شود

اوباما با امضای فرمانی برای تهیه سیاست اجرایی امنیت سایبر از وزارت امنیت داخلی خواست ضمن شناسایی تهدیدات جدید سایبری لایحه جامع اجرای امنیت سایبر در ایالات متحده را تهیه کند. به گزارش ایتنا از خبر آنلاین، این فرمان اجازه می‌دهد تا کمیته ویژه در وزارت امنیت داخله بعنوان نماینده حکومت، اطلاعات ریز در مورد نحوه مشارکت با بخش خصوصی در مورد شناسایی تهدیدات سایبری گرد آوری کرده و همچنین برای توسعه چهارچوبی جدید با استفاده از تجربیات، با هدف کاهش ریسک در حوزه امنیت سایبر گام بردارد. براساس این فرمان دادستان کل، وزیر امنیت داخله، مدیر آژانس امنیت ملی بمدت ۱۲۰ روز وقت دارند تا نحوه پیاده‌سازی موارد مذکور را مدون سازند.

مدیربخش privacy و حقوق دیجیتال مستقر در وزارت امنیت داخله می‌توانند برای جلوگیری از برخورد با حقوق مردم در این باره به تدوین کنندگان مشاوره قانونی دهند. لیست مواردی که باید تهیه شود و همچنین مواردی که نباید مجریان این فرمان در آن دخالت کنند را کاخ سفید در رونوشت جدید خود آورده است. از این فرمان به عنوان دستورالعمل سیاست‌های رییس جمهوری یاد شده تا بخش‌های حیاتی مانند منابع انرژی، مخابرات و ارتباطات و سیستم‌های آبی در اولویت امنیت سنجی علیه تهدیدات جدید سایبری قرار گیرند. اینکه کدام تهدیدات جدی است و ممکن است زیرساخت‌های امریکا مورد حمله واقع شود؛ باید ذیل این حرکت توسط بخش‌های مذکور شناسایی گردد. ❖

به روز رسانی حیاتی اوراکل برای جاوا

روز جمعه اوراکل یک به‌روز رسانی حیاتی برای Java SE عرضه کرد که یک اصلاحیه خارج از نوبت برای دفع سوء استفاده‌هایی که Java Runtime Environment را در مرورگرهای دسکتاپ تحت تأثیر قرار می‌دهند می‌باشد. این اصلاحیه حیاتی که قرار بود روز ۱۹ فوریه عرضه گردد، شامل ترمیم‌هایی برای ۵۰ آسیب‌پذیری است. جاوا اخیراً به دلیل مسائل امنیتی که به‌طور خاص مرورگرها را تحت تأثیر قرار می‌دهند، هدف حمله قرار گرفته است. اوراکل در بولتن خود نوشت: «شهرت Java Runtime Environment در مرورگرهای دسکتاپ و این واقعیت که جاوا در مرورگرها مستقل از سیستم عامل است، جاوا را به هدفی جذاب برای هکرهای خرابکار تبدیل می‌کند.»

۴۴ آسیب‌پذیری از این مجموعه، جاوا را در مرورگرهای اینترنتی تحت تأثیر قرار می‌دهند. به گفته اوراکل این آسیب‌پذیری‌ها فقط در کامپیوترهای دسکتاپ و از طریق برنامه‌های Java Web Start یا اپلت‌های جاوا می‌توانند مورد سوءاستفاده قرار گیرند. به‌علاوه، یک آسیب‌پذیری نیز پروسه نصب کلاینت جاوا (یعنی نصب Java Runtime Environment بر روی کامپیوتر دسکتاپ) را تحت تأثیر قرار می‌دهد. این اصلاحیه حیاتی شامل ترمیم‌هایی که پیش‌تر از طریق هشدار امنیتی CVE-۲۰۱۳-۰۴۲۲ منتشر شده بودند نیز می‌باشد. علاوه بر این‌ها، سه آسیب‌پذیری هر دو نسخه کلاینت و سرور جاوا را تحت تأثیر قرار می‌دهند.

به این تتیب این آسیب‌پذیری‌ها می‌توانند بر روی سیستم‌های دسکتاپ از طریق Java Web Start یا اپلت‌های جاوا و بر روی سرورها از طریق اعمال ورودی خرابکار به APIها در اجزای آسیب‌پذیر مورد سوءاستفاده قرار گیرند.

البته به گفته جاوا در برخی از این نقایص سناریوی سوءاستفاده بسیار غیرمحتمل است. برای مثال، یکی از این آسیب‌پذیری‌ها فقط بر روی سروری مورد سوءاستفاده قرار می‌گیرد که مجوز پردازش فایل‌های تصویری از یک منبع نامطمئن را صادر نماید.

به گفته اوراکل، دو آسیب‌پذیری ترمیم شده در این به‌روز رسانی فقط بر روی نسخه سرور Java Secure Socket Extension اعمال می‌گردند، ولی اغلب آسیب‌پذیری‌های ترمیم شده در این اصلاحیه، نسخه‌های کلاینت جاوا و JavaFX را تحت تأثیر قرار می‌دهند. اوراکل معتقد است که Java server environment امن‌تر از Java Runtime Environment در مرورگرها است، چرا که سرورها در یک محیط امن‌تر و کنترل شده‌تر کار می‌کنند.

Java باز هم در لیست سیاه

اما بعد از این به‌روزرسانی هم شرکت اپل برای دومین بار در طول یک ماه نام ابزار Java ۷ را در لیست سیاه خود قرار داد و گفت که این برنامه تولید شده توسط اوراکل و ابزار به‌روزرسان آن مخصوص سیستم‌عامل Mac حفره امنیتی دارد و ایمن نیست. به گزارش ایتنا، این لیست سیاه جدید بر مبنای یازدهمین به‌روزرسانی نرم‌افزار Java ۷ یعنی آخرین نسخه از این ابزار تنظیم شده است و این دومین بار در طول یک ماه گذشته است که اپل نام این ابزار را در لیست سیاه خود قرار می‌دهد و با استفاده از ابزارهای ضدبدافزاری خود جلوی نصب این نرم‌افزار روی سیستم‌عامل OS X خود را می‌گیرد. هنوز به درستی مشخص نشده است که چرا اپل مجدد این برنامه را وارد لیست سیاه خود کرده است، اما بر اساس گزارشی که به تازگی منتشر شد می‌توان دریافت که بر خلاف تلاش‌های اوراکل مبنی بر ایمن‌سازی Java آخرین نسخه منتشر شده از این برنامه همچنان شامل نقاط آسیب‌پذیر می‌شود. زمانی که اپل برای نخستین بار منع استفاده از Java روی سیستم‌های خود را در ژانویه امسال اعلام کرد، این اقدام از سوی شرکت اپل اندکی غیرمعمول خوانده شد.

در ماه ژانویه شرکت اپل اعلام کرد که دهمین به‌روزرسانی Java ۷ شامل نقاط آسیب‌پذیر فراوانی می‌شود که اگر روی رایانه‌های شخصی این شرکت نصب شود، مشکلات فراوانی را به همراه می‌آورد. اما هم‌اکنون با انتشار یازدهمین به‌روزرسانی این نرم‌افزار، اپل مجددا جلوی استفاده از این ابزار را گرفته است. به تازگی برخی از شرکت‌های امنیتی همچون آویرا نیز از ناامنی Java ۷ خبر داده‌اند. ❖

به‌روزرسانی هوشمند در محصولات آویرا

کارشناسان امنیت آویرا به‌روزرسانی ۳ محصول تحت شبکه خود را اعلام کردند. به گزارش ایتنا از روابط عمومی شرکت آرکا، هدف مشترک در به‌روزرسانی این سه محصول بالا رفتن قابلیت تشخیص بدافزارهای مخرب است، در حالی که در همان زمان کاهش بار سیستم نیز مدنظر قرار گرفته است. به گفته آویرا این محصولات را برای ارزیابی رایگان در دسترس همگان قرار داده شده است.

مهم‌ترین به روزرسانی صورت گرفته در این دوره به‌روزرسانی، استفاده از تکنولوژی حفاظت ابری در Avira Professional Security ۲۰۱۳ و Avira Server Security دو نسخه مهم تحت شبکه آویرا است. استفاده از تکنولوژی حفاظت ابری آویرا برای بهبود روش‌های کلاسیک تشخصی نرم‌افزارهای مخرب انجام شده است. در این تکنولوژی آویرا از سرورهای جدیدی برای آنالیز رفتار بدافزارهای جدید و کشف نشده استفاده می‌شود. استفاده از این روش زمان واکنش به بدافزارها را بسیار پایین می‌آورد. اجرا در ویندوز ۸، بهینه‌سازی‌هایی برای کاهش مصرف منابع سیستمی و جلوگیری از کندی آن و به‌روزرسانی موتور ضدویروس از به‌روزرسانی‌های دیگر محصول حرفه‌ای امنیت آویرا هستند.

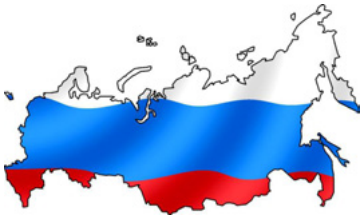
کنسول مدیریت آویرا (Avira Management Console) یکی از مهم‌ترین محصولات این شرکت برای مدیریت امنیت شبکه‌ها است. این ابزار در به‌روزرسانی جدید به نسخه ۲.۷ ارتقا یافته و امکانات بیشتری بر روی آن قرار داده شده است. این نسخه جدید در حال حاضر از محصولات به‌روزرسانی شده در همین دوره پشتیبانی می‌نماید. در نسخه جدید (AMC) این قابلیت ایجاد شده است که در صورت درخواست مدیر شبکه به‌روزرسانی‌های روزانه بسته‌های نرم‌افزاری آویرا به صورت غیرمتمرکز و به طور مستقل از Avira Update Manager انجام شود. این کار برای اطمینان از کاستن ترافیک شبکه در طول به‌روزرسانی بر روی به کامپیوترها متصل به شبکه در دفاتر شعب انجام می‌شود. در نسخه جدید امکان تعریف گروه‌های کاری برای تقسیم کامپیوترهای متصل به شبکه (برای مثال از روی IP آدرس‌ها) فراهم شده است. برای این گروه‌ها تعدادی پیش فرض وجود دارد که کارآیی سیستم را آسان‌تر می‌نماید ولی مدیر شبکه می‌تواند آزادانه این گروه‌ها را تغییر داده و یا تشکیل دهد. با به‌روزرسانی‌های جدید انتقال تنظیمات کامپیوترهای شبکه به وجود آمده است. همچنین می‌توانید تنظیمات گروهی خود را به Avira Management Console منتقل نمایید. رایان سامانه آرکا به عنوان نماینده انحصاری محصولات آویرا با پشتیبانی مناسب توانسته محصولات به‌روز و با تکنولوژی بالای کشور آلمان را به صورت قانونی و رسمی در اختیار کارشناسان و مهندسان ایرانی قرار دهد. ❖

هرزنامه‌ای با سوءاستفاده از شبکه اجتماعی LinkedIn

تیم فنی آویرا هرزنامه‌ای را شناسایی نموده است که از نام شبکه اجتماعی - کاری LinkedIn برای تبلیغ وب سایت داروخانه آنلاین سوءاستفاده می‌کند. به گزارش ایتنا از شرکت آرکا، این ایمیل تظاهر می‌کند که از "بخش پشتیبانی فنی LinkedIn" یا "بخش مدیریت سایت LinkedIn" و یا از "بخش یادآوری LinkedIn" برای کاربران این شبکه اجتماعی ارسال شده است. این اسپم جدید پیام کوتاهی برای کاربر شبکه اجتماعی Linkedin دارد و کاربر را به باز کردن لینکی که در ابتدای آن آدرس www.linkedin. com مشاهده می‌شود، ترغیب می‌نماید. این هرزنامه بسیار مشابه اسپمی است که چندی پیش نیز چنین سوءاستفاده‌ای را انجام داده بود. در همه ایمیل‌های بررسی شده مشاهده شد که این سیستم از آدرس ایمیلی استفاده می‌کند که جعلی نیست ولی IP آدرس‌های استفاده شده منحصربه‌فرد است، که این نشانه‌ای روشن است که متقلب باتنت بزرگی را برای ارسال این ایمیل ها در اختیار گرفته است. این واقعیت حتی جالب‌تر این است که میزبان سرور SMTP تقریبا تمام دامنه‌ها بسیار مشکوک است و بسیاری از آنها را در روسیه (یا کشورهای روسی‌زبان) می‌باشد. هر چند دامنه‌هایی دیده شده که آلمانی هستند و یا و از IP آدرس‌های آلمانی استفاده نموده‌اند. تیم فنی شرکت رایان سامانه آرکا نماینده رسمی آویرا در ایران به تمام کاربران توصیه می‌کند برای جلوگیری از کلاهبرداری مجرمان اینترنتی چنین ایمیل‌های مشکوکی را بلافاصله حذف نمایند. ❖

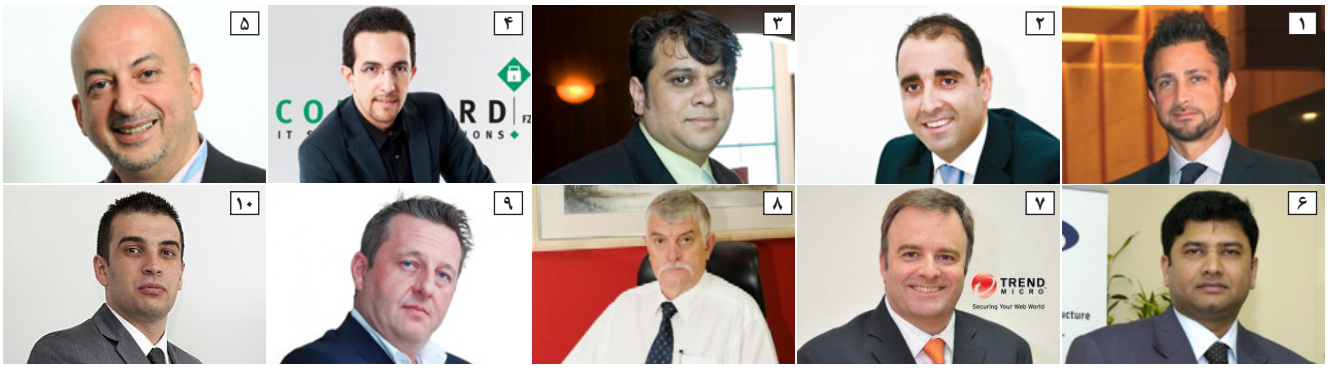
دفاع سایبری روسیه تقویت می‌شود

رییس‌جمهور روسیه به دنبال کشف رخنه یک شبکه جاسوسی به رایانه‌های دولت و سفارتخانه‌های این کشور، دستور حفاظت از رایانه‌های دولتی در برابر حمله‌های هکری را صادر کرد. به گزارش ایتنا بر اساس این فرمان که ولادیمیر پوتین آن را در ۱۵ ژانویه امضا کرده است که به سرویس امنیت فدرال (FSB) اختیار می‌دهد یک سیستم ملی برای شناسایی، پیشگیری و نابودی تاثیر حملات رایانه‌ای به منابع اطلاعات فدراسیون روسیه ایجاد کند. شبکه جاسوسی که اکتبر سرخ نام گرفته از حملات فیشینگ (ایمیل‌های ناخواسته به هدف‌های مشخص) به یک برنامه جمع‌آوری اطلاعات و ارسال آنها به یک سرور استفاده کرده است. طبق این حکم که در وب سایت کرملین منتشر شد، رایانه‌های دولتی و شبکه‌های مخابراتی که توسط سیستم امنیت سایبری محافظت می‌شوند باید شامل رایانه‌های داخل و سفارخانه‌ها و کنسولگری‌های خارج از کشور باشند. چندی پیش شرکت روسی Kaspersky اعلام کرده بود که شبکه جاسوسی رایانه‌ای را در اکتبر گذشته کشف کرده است. این شبکه از سال ۲۰۰۷ به دنبال کسب اطلاعات از کشورهای اروپای شرقی و همچنین جمهوری‌های شوروی سابق شامل روسیه بوده است.



یک کارشناس ویروس‌های رایانه‌ای در کاسپرسکی اظهارکرد که بسیاری از سیستم‌های آلوده شده، متعلق به هیأت‌های دیپلماتیک بودند. به گزارش رویترز این کارشناس هفته گذشته گفته بود که این شبکه جاسوسی همچنان فعال است و کشورهای اروپایی متعددی در حال بررسی آن هستند. ❖

۱۰ مدیر برتر امنیتی خاورمیانه



ماهنامه Channel هر ساله گزارشی با عنوان Channel Champions 50 منتشر می‌کند که در آن بر فعالیت‌های مدیران اجرایی شرکت‌هایی تاکید دارد که نقش مهمی را در توسعه بازار فناوری اطلاعات خاورمیانه ایفا می‌کنند و اقدامات آنها جامعه شبکه توزیع را از طریق برداشتن گام‌های بیشتر تحت تاثیر قرار داده است.
گزارش Channel Champions 50 در پنج بخش تقسیم‌بندی شده است که در هر بخش ۱۰ مدیر برتر و موفق در منطقه خاورمیانه معرفی شده است، آنچه در ادامه می‌خوانید خلاصه از گزارش مفصل این ماهنامه در معرفی ۱۰ مدیر برتر و موفق حوزه امنیت در خاورمیانه است:

۱- رمزی ایتانی، مدیر هماهنگی و کانال منطقه، سیمانتک MENA

سیمانتک در حال تحول است ولی‌ایتانی همچنان کانال را در دست دارد. این کمپانی با چالش‌های جهانی روبروست. نظیر تلاش سخت برای تبدیل استراتژی خود از مدل کسب‌وکاری که تکیه بر فروش لیسانس نرم‌افزارها و سخت‌افزارهای خرد دارد به مدل SaaS که درآمدی متداوم برای کمپانی و اعضای کانال دارد. نظر به امکاناتی که در رایانش ابری و ارتباطات سیار به همراه دارد ایتانی و اعضای کانال سعی می‌کنند راه‌حل‌های درستی را پیدا کنند که درآمد متداومی برای همکاران و اعضا به همراه داشته باشد.

۲- خاویر حداد، مدیر کانال EMC

ای ام سی هم چنان می‌کوشد برنامه همکاران Velocity را تقویت کند. حداد به تازگی بسته تازه‌ای در حوزه شایستگی خدماتی برای توزیع‌کنندگان ولوسیتی آماده و رونمایی کرده است و با جذب همکاران آموزش‌دیده و کسب مجوز برای توزیع محصولات باکیفیت، سعی داشته تا خدمات اسمبلی به همکارانش ارائه کند.

۳- امان منظور، مدیر کانال لابراتور کسپرسکی در خاور میانه

کسپرسکای سعی می‌کند در سال ۲۰۱۴ بهترین فروشنده امنیت سیستم‌های کامپیوتری شود و هم چنین کسب‌وکار MEA را رونق بدهد. منظور سعی می‌کند اسباب ارتباط بین فروشنده اصلی از سویی و فروشنده فرعی و مامورین توزیع از سوی دیگر باشد تا راه‌حل‌هایی که به بازار ارائه می‌کند هم چنان ارزشمند باقی بماند.

۴- محمد مبصری، قائم مقام کامگارد

کامگارد یکی از تخصصی‌ترین کمپانی‌های ایجاد راه‌حل‌های امنیتی در حوزه IT است و متخصصین بسیاری در زمینه فروش خدمات امنیتی در آن حضور دارند که مایلند وارد فضای SI و ایجاد راه‌حل شوند. مبصری مهم‌ترین حلقه ارتباط فروشندگان و استراتژی توسعه کمپانی در منطقه است که کسب‌وکار پولسازی را برای همکارانش شکل می‌دهد.

۵- عمر برکات، مدیر حوزه، کشورهای شام و شمال آفریقا، مکافی MENA

مکافی از زمانی که زیر چتر کمپانی اینتل قرار گرفته است همچنان سعی دارد همچون گذشته راه‌حل‌های امنیت IT را رشد بدهد. برکات با تخصص منطقه‌ای گسترده‌ای که دارد می‌کوشد کمک کند ابعاد مختلف تکنولوژی پلتفرم دیپ‌سیف ساخت اینتل را برای هم کارانش روشن بکند. او هم چنان در راه‌اندازی چندین برنامه مختلف کانال نقش داشته است.

۶- شاه‌نواز شیخ، مدیر منطقه ای دل سونیک وال

اگر کسی بخواهد در کانال IT امروز موفقیت به دست بیاورد باید چندین توانمندی هم زمان داشته باشد و شیخ یک نمونه از این گونه افراد است. وی نه تنها اکوسیستم هم کاری کمپانی را ثبات بخشیده است بلکه کانال قدیم سونیک وال را به قدری توسعه داده است که تمام همکاران دل را دربربگیرد.

۷- کریس مور، مدیر کل‌ترند میکرو MEA

او مسوول راه‌اندازی اصلاحات بزرگ در برنامه کانال بوده است و تمام تلاشش معطوف به این است که همکارانش در منطقه ببینند برای هر اقدامی چه شرایطی مورد نیاز است. ترند برنامه‌هایش را اصلاح کرده است تا مدل مدیریتی خود را تغییر بدهد.

۸- کریس کرنلیوس، قائم مقام، فروش و پشتیبانی، تک اسس

این چهره پس از مدیریت اجرایی MENA در Sunبه این جایگاه تازه در تک اسس روی آورده است و آن سابقه درخشان اوضاع فعلی وی را تضمین می‌کند. او در موقعیت قائم مقام نه تنها خود را وقف فروش کرده است بلکه در راه‌اندازی بسیاری از اقدامات جدید تک اسس هم نقش کلیدی داشته است.

۹- لی رینولدز، مدیر عامل کمپانیMEA و APAC

کامپیوترلینکس یکی از توزیع‌کنندگان محلی گسترده‌ترین خدمات تراز اول امنیت IT در منطقه است و سعی می‌کند تمرکز خود را بر راه‌حل‌ها افزایش بدهد. این شرکت سعی می‌کند با استفاده از راهنمایی‌های رینولدز جای پای خود را در منطقه محکم کند و تا جایی که ممکن است ارزش بیشتری به شرکت‌ها بیفزاید.

۱۰- خالد معاشر، مدیر توسعه کسب و کار بیت‌دیفندر

بیت‌دیفندر سعی می‌کند کانال را در MENA رشد بدهد و به همین دلیل به توسعه کسب‌وکار اهمیت بسیاری می‌دهد. معاشر نقطه تماس محلی اکوسیستم کانال در منطقه است و نقش مهمی در رشد برند بیت‌دیفندر و خروج آن از گمنامی داشته است. ❖

مکانی برای تلاقی امنیت و رایانه

معرفی شرکت امنیتی ESET

بسیاری از ما برای انتخاب نسخه ضدویروس برای نصب روی کامپیوتر خود دچار مشکل و در مراجعه به متخصصان و یا مراجعه به مراکز خرید با اسامی مختلفی روبرو می‌شویم که هر یک به زعم خود مزایا و معایب خاصی دارند. ولی در این میان نام‌هایی وجود دارند که در میان عامه جامعه به خوبی آشنا هستند. برای مثال کمتر کسی در دنیای امروز را می‌توان یافت که با نام ضد ویروس‌های سری نود "Nod" آشنا نباشد. شاید بسیاری از افراد ندانند که این محصولات توسط یک شرکت بزرگ به نام ESET تولید می‌شوند. در این مقاله قصد داریم تاریخچه مختصری از این شرکت اروپایی را برای شما روایت کنیم.

غول کشی از بلوک شرق

ESET یک شرکت امنیتی مطرح در حول محور آی‌تی است که مقرش در شهر براتیسلاوا، پایتخت کشور اسلواکی قرار دارد. در سال ۱۹۹۲ میلادی بود که از تلفیق و ادغام دو شرکت خصوصی کوچک نخستین پایه‌های این شرکت شکل گرفت و بر همان اساس شرکت امروزی ESET تاسیس گردید. طرح‌ها و چشم اندازهای "است" از ابتدا بسیار بزرگ و چشم‌گیر طراحی شده بودند. به همین سبب زمان زیادی طول نکشید تا این کمپانی به موفقیت‌های درجه یک در سطح بین‌المللی دست یابد و در مدتی کمتر از بیست سال نام ESET به عنوان یکی از ۵ نرم‌افزار امنیتی برتر جهان آوازه یابد. به طوری که در سال‌های ۲۰۰۸، ۲۰۰۹ و ۲۰۱۰ نشان موفق‌ترین شرکت اسلواکی را از آن خود کرد.

این شرکت که به صورت کاملا خصوصی اداره می‌گردد، علاوه بر شعبه مرکزی از شعبه‌های دیگری در نقاط جهان برخوردار است که از این میان می‌توان به شعبه‌های سن دیگو و کالیفرنیا در ایالات متحده آمریکا، مونترال در کشور کانادا، بوئنوس آیرس پایتخت آرژانتین، پراگ جمهوری چک، کراکوف لهستان و سنگاپور اشاره نمود. البته این نمایندگی‌ها تنها قطب‌های اجرایی ESET به حساب می‌آیند. در زمینه فروش سطح کاری شرکت بسیار گسترده‌تر است. تا جایی که امروزه امکان پخش محصولات ESET در بیش از ۱۸۰ کشور جهان وجود دارد. امروزه دفتر اصلی این شرکت و تمامی شعبه‌های آن در سطح جهانی دارای بیش از ۸۰۰ کارمند است.

در دسامبر سال ۲۰۱۰ "است" از انتصابات جدیدی در راستای بهبود خدمات و بالا بردن کیفت خدمات و محصولات خبر داد که شامل انتصاب ریچارد مارکو (Richard Marko) به عنوان مدیر اجرایی در سطح بین‌المللی (Global CEO)، میلان ماساریک (Milan Masaryk) به عنوان مدیر ارشد مالی (CFO)، پاول لوکا (Pavol Luka) به عنوان مدیر ارشد فناوری (CTO)، ژوراژ مالکو (Juraj Malcho) به عنوان مدیر ارشد تحقیقات، ایگناسیو اسباماپاتو به عنوان مدیر فروش و بازاریابی در سطح جهانی، اندرو لی (Andrew Lee) به عنوان مدیر عامل شرکت در شعبه شمال آمریکا بودند. در راستای این تغییرات بنیانگذاران شرکت نیز به عنوان هیئت مدیره و بدنه اصلی این کمپانی مشغول به کار شدند. یکی از فعالیت‌های مهم این شرکت ارائه راه حل‌های امنیتی در برابر تهدیدات اینترنتی است که به طور قابل توجهی نیز در حال پیشرفت است.

نخستین گام‌های پیشرفت

تاریخ آغاز به کار ESET به سال ۱۹۸۷ میلادی باز می‌گردد؛ زمانی که دو برنامه نویس جوان و مشتاق با نام‌های پیتر پاسکو (Peter Paško) و میروسلاو ترنکا (Miroslav Trnka)، نخستین ویروس کامپیوتری را کشف کردند و لقب "وین" را به آن دادند. سپس برنامه‌ای برای ردیابی این عنصر مزاحم کامپیوتری نوشتند. در ادامه این رخداد مدت زمان کمی طول کشید تا تعداد زیادی ویروس کشف شد و همین موضوع زمینه‌ساز جرقه خوردن ایده‌هایی در زمینه راه‌حل نرم‌افزاری فراگیر برای مقابله با تهدیدهای یارانه‌ای ناشناخته گردید.

در سال ۱۹۹۲ این دو دوست با همکاری متقابل با رودلف هروبای (Rudolf Hrubý) ESET را به عنوان یک شرکت خصوصی با مسئولیت محدود تاسیس کردند.

این گروه جوان به تدریج به نوشتن برنامه‌های آنتی ویروس قوی‌تر و گسترده‌تر پرداختند و به حدی در این کار پیشرفت کردند که به یکی از سریع‌ترین و موثرترین برنامه‌های آنتی ویروس در سطح جهان دست یافتند و برنامه‌هایشان به سرعت محبوبیت بالایی را در میان کاربران این دست نرم‌افزارها کسب کرد. در طول روند رشد و پیشرفت شرکت ESET همه به اصول اصلی و فلسفه وجود شرکت که از ابتدا بین موسسان آن تنظیم شده بود پایبندی کامل داشتند. این قوانین شامل مسئولیت، قابلیت اطمینان، درستکاری و صداقت بودند که به سادگی به بستری برای ایجاد نوآوری در شرکت تبدیل شدند و به همراه طبع جاه طلب این گروه به رشد و پیشرفت شرکت در سطح جهانی منجر شد. زیرا مهندسی و اداره کردن مجموعه برای سرعت و پایداری بیشتر و برآورده ساختن خواسته‌های بنیانگذاران با فناوری‌های پیشرفته به نوعی دفاع از کاربر کامپیوتر نیز به حساب می‌آید.

اگر بخواهیم پیشرفت‌های سالانه شرکت را بررسی کنیم، می‌توانیم به اختصار به موارد زیر اشاره نماییم:

در سال ۱۹۹۹ میلادی شعبه مشارکت خارجی نامحدود ESET در سن دیه گو امریکا گشایش یافت که مهم‌ترین گام شرکت در جهانی شدن محسوب می‌گردید.

تاسیس شـرکت نرم‌افزارESET در شهر پراگ پایتخت جمهوری چک در سال ۲۰۰۱ به وقوع پیوسـت تا جایـگاه این کمپانی در شـرق اروپا مستحکم‌تر گردد.

در سال ۲۰۰۲ نخستین مشارکت این شرکت در نمایشـگاه سـبیت هانوفر آلمان بـه انجام رسـید تا در یکی از مهم‌ترین بسترهای معرفی محصولات و فناوری‌های کامپیوتری، خود را به اثبات برساند.

پخش گسـترده آنتی ویروس NOD32 و نیز توضیع برنامه امنیتی هوشـمند ۳,۰ (Smart Security 3.0) از سـوی شرکت ESET در سـال ۲۰۰۷ صورت گرفت که محبوبیت این شـرکت را در سـطح بالایی در میان کاربران بالا برد.

در سـال ۲۰۰۸ پژوهشـکده و مرکز توسعه و پیشـرفت این شرکت در لهسـتان آغاز به کار کرد تـا گسـترههای نوینی بـرای کارکرد شرکت ایجاد گردد.

شـعبه دیگری از پژوهشکده و مرکز توسـعه و پیشرفت شـرکت ESET در مونترال کانادا در سـال ۲۰۱۲ گشـایش یافت تا محصـولات بر اسـاس نیازهای یکی از مهم‌ترین بازارهـای نرم‌افزارهـای امنیتـی یعنـی منطقه آمریکای شـمالی نیز تطبیق یابند.

روند تکاملی محصولات

در سال ۱۹۹۸ میلادی نخستین محصول شرکت ESET به بازار وارد شد که برنامه آنتی ویـروس NOD نام گرفتـه بود و بر روی کامپیوترهای دارای سیسـتم عامل MS- DOS اجرا می‌شـد. پس از این محصـول بود که این شـرکت در سـال ۲۰۰۳ آنتی ویروس NOD32 1.0 را وارد بازار کـرد. این محصول از این جهت بسـیار مهم و قابـل توجه بود که برای نخسـتین بار بر روی سیسـتم عامـل ویـنـدوز مایکروسـافت مورد اسـتفاده قرار می‌گرفت. پس از مدت کوتاهی آنتـی ویروس NOD32 2.0 به دنبال نسـخه پیشین وارد بازار شد که نقطه عطفی در عملکرد این شـرکت به حساب می‌آمد. در نوامبر سال ۲۰۰۶ آخرین انتشـار کدهای این سری با نام مخفـف 2.70.39.2 x انجام گرفت و در ماه می سال ۲۰۱۲ پشتیبانی از این سیستم به طور کلی قطع شد.

در سـال ۲۰۰۷ این شرکت، نسخه شماره ۳,۰ از آنتی ویروس NOD32 را منتشـر ساخت و پس از آن برنامه امنیت هوشمند ۳,۰ (Smart Security 3.0) کـه محصولی از ترکیب آنتی ویـروس NOD32 بـا سیسـتم آنتی اسـپم و فایـروال بود را وارد بازار نمـود که به صورت کامـل در تمام زمینه‌ها امنیـت کامپیوتر را به عهده می‌گرفت.

در مـارس سـال ۲۰۰۹ نسـخه 4.2 از آنتی ویـروس NOD32 و برنامه امنیت هوشـمند (Smart Security) انتشـار یافـت. آنتـی ویـروس NOD32 و برنامه امنیت هوشـمند 4.2 (Smart Security 4.2) هر دو بر روی سیستم عامل‌های به روز دنیا مانند ویندوزهای Windows 2000, , Server 2003, Server 2003 R2, Vista, Server 2008, Server 2008 R2 قابـل اجـرا بود و مدتی بعـد در یک پکیج تکمیلی امکاناتی به این آنتی ویروس اضافه گردید که از سیسـتم‌های عامل Microsoft Windows NT 4.0 with Service Pack 6a پشتیبانی می‌نمود. هر دو نوع ۶۳ بیتی ۳۲ بیتی این سیسـتم‌های عامل نیز در فهرسـت پشـتیبانی این شـرکت جای گرفته بودند.

کاربران نسخه‌های قدیمی ویندوز مایکروسافت هماننـد ویندوزهـای ۹۵، ۹۸، Me و NT 4.0 نیاز به نصب نسـخه قدیمی 2.70.39 داشتند. علاوه بر این گروه ویندوزهای مایکروسـافت از سیسـتم عامل‌هـای BSD, Linux, Mac OS X, Novell NetWare و Sun Solaris پشتیبانی می‌نمود.

در سپتامبر سـال ۲۰۱۰ ESET آنتی ویروس NOD32 را برای نسـخه تجـاری Mac OS X روانه بازار کرد و در نوامبر همین سـال یک نسخه از سیسـتم اصلی امنیت سایبر نیز برای Mac OS Xمنتشر ساخت.

در ماه می سـال ۲۰۱۱ این شرکت تست بتای آنتـی ویـروس NOD32 و نسـخه ۵ امنیت هوشـمند در سطح عمومی را آغاز کرد و امکان به روز رسانی و ارتقا بخشیدن رایگان نسخه‌های پیشـین را که تا به امروز سـطح جهانی انتشار داده شـده بود در سراسر دنیا ایجاد کرد. قابل توجه است که این سـرویس رایگان برای همه آنتی ویروس‌های NOD32 اسـت و دارندگان مجوز هوشـمند x.4 نسـب به دیگـر کاربران زودتر و آسان‌تر توانستند به آن دست یابند.

پـس از آن پیشـرفت قابـل توجهـی در آنتی ویروس NOD32 و نسـخه ۵ امنیت هوشمند ایجاد شـد که توانایی کنترل و بررسـی کردن USB، هارد اکسترنال، درایوهای CD/DVD را دارد و هرگونـه ویروس و تهدید و ... را تحت کنترل قرار می‌دهد.

یکـی از نکات قوت مهم ESET این اسـت که محدوده محصولات این شـرکت از نسخه‌هایی از برنامـه امنیت تلفـن همراه بـرای کاربران ویندوزهـای موبایـل، اندروید و سـیمبین نیز برخوردار اسـت و این دسته از آنتی ویروس‌ها علاوه بر حفاظت در برابر نرم‌افزارهای مخرب، حفاظت در برابـر پیام‌های کوتاه SMS مخرب را نیز فراهم می‌کند. همچنین دارای سامانه‌های firewall و ویژگی‌های ضد سرقت، مانند قفل شدن سیم‌کارت و یا سیستم پاک کردن موارد و اطلاعات خصوصی از راه دور است. ❖

تهدیدات امروز، ابزار به‌روز

یاشار بهمند
behmand@ccwmagazine.com

از آغاز پیدایش دولت‌ها در حدود ۵۰۰۰ سال پیش، فعالیت‌های نظامی در بیشتر جهان به وقوع پیوسته است. اما در طی تاریخ دکترین و استراتژی نظامی به خاطر خط‌شکنی‌های انقلابی در فناوری، دستخوش تغییرات عمیق شده‌اند. فناوری‌های نوین به صورت یک سلاح جدید، یک منبع انرژی جدید یا یک وسیله ارتباطی جدید، همگی موجب شده‌اند که نوآوران از جنگ فرسایشی پرهیز کرده و در عوض با استفاده از این فناوری‌ها جنگ را متحول کنند.

همان اندازه که فناوری‌های پیشین چون ساخت باروت، TNT، پرواز، اتمی و ... باعث سرعت گرفتن روند توسعه فناوری‌های نظامی شد، باید گفت که رشد خیره کننده فناوری اطلاعات و ارتباطات، موج پرقدرتی است که ماهیت و ویژگی‌های جنگ و منازعه را از بیخ و بن تغییر داده است.

اگر میدان نبرد در سال‌های نه چندان دور محدود به یک منطقه بود، امروز کل دنیای مجازی در محدوده منطقه خطر قرار دارند و خطر و ناامنی تمامی افرادی را که به هر نحو با این فناوری مرتبط است را تهدید می‌کند. همچنان هدفشان آسیب زدن به شماست ولی این بار می‌دانند اطلاعات شما اهمیت بسیار دارد و قصد حملات این بار اطلاعات شماست!

«جنگ اطلاعاتی» یک اصطلاح نسبتاً جدید است که طی سال‌های گذشته به واژه‌نامه اصطلاحات نظامی وارد شده است. ظهور اصطلاح جنگ اطلاعاتی و اهمیت روزافزون آن احتمالاً با انقلاب اطلاعات ارتباط مستقیم دارد. «انقلاب اطلاعات» آن قدر قدرتمند و دامنه تاثیر آن، به قدری گسترده است که می‌تواند بعد جدیدی در جنگ یا اصلاً سبک جدیدی از جنگ را تعریف کند. جنگ اطلاعاتی یعنی کاربرد اطلاعات و سیستم‌های اطلاعاتی به عنوان یک سلاح در درگیری‌هایی که اطلاعات و سیستم‌های اطلاعاتی یک هدف نظامی مهم به شمار می‌روند.

اگر از بستر ICT استفاده شود، می‌توانیم از عنوان این نوع جدید نبردها با عنوان «جنگ سایبری» استفاده نماییم. جنگ سایبری یعنی نفوذ در سیستم‌های اطلاعاتی و ارتباطی که دشمن برای «دانستن» خود به آنها تکیه می‌کند، یعنی اینکه او کیست؟ کجاست؟ چه کاری را در چه زمانی می‌تواند انجام دهد؟ چرا می‌جنگد؟ چه تهدیداتی در اولویت قرار دارند؟

در جنگ سایبری تلاش می‌شود تا همه چیز را درباره دشمن بدانیم و در عین‌حال نگذاریم او هیچ چیزی درباره ما بداند. به بیان دیگر، هدف اصلی در جنگ سایبری بر هم زدن «موازنه اطلاعات و دانش» به نفع نیروهای خودی است. بنابراین در جنگ سایبری می‌توان با بهره‌گیری از دانش برتر، ضعف سرمایه و نفرات کمتر را جبران کرده و به پیروزی قاطع دست یافت.

در سال‌های اخیر جنگ‌های سایبری روی دیگر خود را نیز به ما نشان داده است. این بار هدف نه تنها کسب اطلاعات، بلکه تخریب تجهیزات است. در سال‌های گذشته شاهد این حملات در کشور خودمان بودیم. برای مثال «استاکس‌نت» هدفمند و به منظور خرابکاری سیستم‌ها در برخی از سازمان‌های ایرانی طراحی شده بود.

جنگ سایبری می‌تواند بین دولت‌ها یا از برخی جهات حتی بین بازیگران غیردولتی اتفاق افتد. هدف می‌تواند نظامی، صنعتی، غیرنظامی یا حتی فضای سروری باشد که مطمئناً به مشتریان بسیاری خدمات ارائه می‌دهد.

البته این روزها جنگ‌های اطلاعاتی و سایبری فقط بین دو کشور رخ نمی‌دهد و در مقیاس‌های کوچک‌تر حتی می‌توان نمونه‌هایی از این جنگ را در بین دو شرکت رقیب مشاهده نمود. بارها شاهد ربودن متن نرم‌افزارها در بین رقبای تجاری بوده‌ایم. این بار هدف اطلاعات شرکت است و نتیجه به بار آمده، شکست‌های تجاری شرکت‌هایی است که اصول اولیه امنیتی این جنگ‌ها را رعایت نمی‌کنند.

حتی نمونه‌ای از جنگ‌های سایبری امروز در بین افراد خاطی و نیروهای امنیتی چون پلیس در هر کشوری در جریان است. هر روز تعداد افرادی که از بستر ICT برای تهدید، دزدی، کلاهبرداری و حتی جنایت استفاده می‌کنند، بیشتر و بیشتر می‌شود.

چه به این تهدیدات از بعد جنگ‌های نظامی و سایبری و از نگاه تهدیدات بین‌المللی نگاه کنیم و چه در ابعاد کوچک‌تر آنها را نوعی رقابت تجاری تلقی نماییم و چه به عنوان یک کاربر عادی خود را در مقابل تهدیدات هکرها و کلاهبرداران اینترنتی تصور کنیم، باید برای حملاتی که دیگر وابسته به زمان و مکان نیستند و هر آن اطلاعات ما را تهدید می‌کنند، به فکر راه چاره باشیم.

خوشبختانه در این جنگ ما تنها نیستیم و سپرهای امنیتی و دیوارهای مستحکمی هستند که چه بسا بسیاری از افراد یک جامعه، کشور و حتی یک جهان به آن‌ها دلگرم هستند. در دنیای امروز شرکت‌های امنیتی سهم مهمی از وظیفه خطیر مقابله با تهدیدات را بر عهده گرفته‌اند. این شرکت‌ها ابزارهای گوناگونی تولید نموده‌اند تا ما امن‌تر باشیم و در این دنیای پرتهدید بتوانیم از فرصت پیش آمده به واسطه «انقلاب اطلاعات» بهره کافی را ببریم. در جنگ میان خیر و شرهای فضای مجازی این شرکت‌های امنیتی در بین دوستان ما قرار دارند.

کاربران رایانه‌ای باید ضمن هوشیاری و رعایت نکات امنیتی، می‌توانند سیستم‌های خود را به ابزارهایی مجهز نمایند که این شرکت‌ها در اختیار ما قرار داده‌اند. ضدویروس، ضد اسپم و دیواره‌های آتش چند نمونه از محصولاتی هستند که می‌توانند کمک شایانی در شناسایی و نابودی بخشی از این تهدیدات نماید.

اما آنچه در این بین اهمیت دارد، شناخت صحیح این نرم‌افزارهای امنیتی و استفاده مناسب از آنهاست. امروزه نسخه‌های اصلی بسیاری از این محصولات در کشور ما و به صورت قانونی و با کدهای به روزرسانی اصلی ارائه می‌شود. توان بالای شرکت‌های امنیتی بین‌المللی وقتی در کنار دانش متخصصان ایرانی نمایندگان آنها قرار می‌گیرد، اطمینان قلبی به ما می‌دهد تا با حضور در این فضای خطرناک ICT بتوانیم از ابزارهای این فناوری نوین برای بهبود زندگی خود بهره بجوییم.

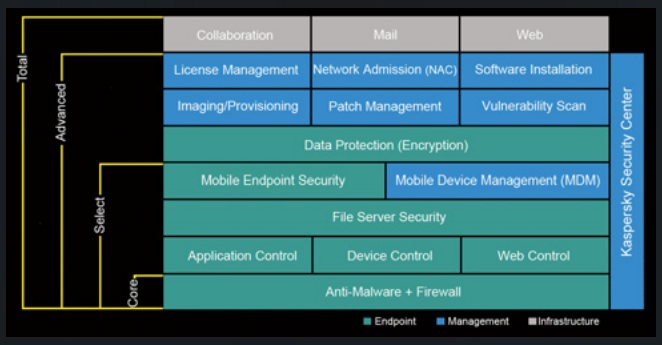
البته باید مراقب باشیم تا در دام‌هایی نیفتیم که در این راه برای ما پهن شده است. چه بسا دوستانی از روی نادانی و یا برخی فقط برای کسب سود با اطلاعات ارزشمند ما بازی کنند! ❖

رونمایی از راهکار ایده‌آل کسپرسکی برای سازمان‌ها

از راهکارهای جدید سازمانی شرکت کسپرسکی با نام **Kaspersky Endpoint Security for Business**، همزمان با سایر کشورهای دنیا، در ایران رونمایی شد. به گزارش ایتنا از روابط عمومی پاد، گل‌مر بحری مدیرعامل شرکت پارس آتنا دژ (پاد) و نماینده رسمی توزیع محصولات کسپرسکی در ایران با اعلام این خبر گفت: این راهکارها ۳۱ ژانویه (۱۲ بهمن) به بازارهای دنیا عرضه و جایگزین محصول قبلی سازمانی کسپرسکی با عنوان **Kaspersky Open Space Security** شد.

مدیرعامل پاد یکی از مهم‌ترین تفاوت‌های این محصول با محصول پیشین را استفاده از **Activation Code** برای فعال‌سازی محصول به جای **License** دانست. به این ترتیب سازمان‌ها می‌توانند به آسانی به مدیریت و کنترل یکپارچه و شفاف تعداد مجوزهای استفاده از نرم‌افزار پرداخته و از سواستفاده دیگران خارج از سازمان جلوگیری کنند. وی در مورد تفاوت‌های این محصول با دیگر محصولات مشابه گفت: کسپرسکی در محصول جدید خود، به خوبی پا را از یک آنتی‌ویروس فراتر گذاشته و راهکار امنیتی جامع و فراگیری برای حفظ امنیت شبکه و اطلاعات سازمان‌ها ارایه کرده است. این محصول در چهار نسخه اول هر کدام برای گروه خاصی از مشترکان طراحی شده است.

گروه اول به نام **Core** برای سازمان‌هایی مناسب است که صرفاً به دنبال راهکاری سبک به عنوان آنتی‌ویروس و مدیریت مرکزی برای سیستم‌های کاربری هستند. نسخه دوم به نام **Select** روانه بازار می‌شود. با توجه به نیازهای امنیتی سازمان‌های ایرانی، انتظار می‌رود بیشترین طرفدار را داشته باشد. امنیت جامع ایستگاه‌های کاری و سرورهای فایل، کنترل و تهیه فهرست برنامه‌های مورد اعتماد، کنترل دستگاه‌ها و کنترل وب، مرورگر امنیتی و سیستم



مدیریت دستگاه‌های موبایلی از جمله امکانات این محصول است. محصول **Advanced** نسخه سوم این محصولات است این محصول علاوه بر امکانات نسخه‌های پیشین، با امکاناتی مانند رمزگذاری و **System Management**، به مدیریت امنیت سیستم‌های کاربری به صورت غیرمستقیم می‌پردازد. اما نسخه **Total** کسپرسکی، کامل‌ترین محصول سازمانی این شرکت است که علاوه بر بهره‌مندی از امکان تمام نسخه‌های پیشین، امنیت کاربران را در سرورهای اینترنت، ایمیل و **Collaboration** فراهم می‌کند. این راهکار برای سازمان‌هایی که نیازهای امنیتی گسترده در لایه سرور و درگاه‌های ورودی شبکه دارند، پیشنهاد می‌شود.

مدیرعامل پاد تاکید کرد: کسپرسکی بزرگترین شرکت خصوصی ارایه کننده راهکارهای امنیتی شبکه و اطلاعات است و به هیچ دولتی وابسته نیست. از سوی دیگر این شرکت در ایران نماینده رسمی دارد و این رابطه مستقیم سبب شده مخاطرات و تهدیدات علیه سازمان‌های ایرانی را با سرعت بسیار زیاد شناسایی کرده و در مقابل آنها عکس‌العمل نشان دهد.

محصول جدید کسپرسکی

پاسخگویی به تمام نیازهای امنیتی

گفت‌وگوی دنیای کامپیوتر و ارتباطات با گل‌مر بحری، مدیر عامل شرکت پارس آتنا دژ

وقتی خبر انتشار نسخه جدید کسپرسکی و بررسی آن در جلسه تحریریه ماهنامه مطرح شد، تصمیم گرفتیم تا پیرامون چند نکته که برای ما مبهم بود با خانم گل‌مر بحری، مدیرعامل شرکت پاد، مصاحبه‌ای داشته باشیم تا به طور صریح سوالاتمان را از وی بپرسیم. مصاحبه پیش رو نتیجه این پرسش و پاسخ است و امیدواریم پاسخی بر پرسش‌های شما دوستان نیز باشد.

رابطه پاد با کسپرسکی چیست و به چه دلیل شرکت شرکت پارس آتنا دژ تصمیم گرفت تنها نماینده کسپرسکی در ایران باشد که این محصول را همزمان با سایر کشورهای دنیا، درایران رونمایی نماید؟

شرکت پاد توزیع کننده رسمی محصولات کسپرسکی است و در بالاترین سطح نمایندگی کسپرسکی (VAD) و به عنوان سرشاخه فروش محصولات تحت شبکه کسپرسکی در ایران فعالیت می‌کند. این شرکت به تمامی نمایندگان سطح بالای خود در سراسر جهان، رونمایی این محصول را اعلام کرده بود. و طبعا پاد نیز به همین دلیل به طور گسترده و پررنگ به رونمایی و معرفی این محصول در سطح کشور پرداخت. از جمله فعالیت‌های ما برای رونمایی این محصول نیز انتشار اخبار، مقالات و آگهی در رسانه‌های معتبر حوزه، انتشار وسیع بروشورهای محصول جدید در سطح کشور با همکاری شبکه نمایندگان، برگزاری مسابقه بزرگ پیامکی در میان مشتریان و... بوده است.

در خبرها از سوی شما اعلام شده بود که این محصول جدید جایگزین محصول قبلی سازمانی کسپرسکی شده است، آیا Kaspersky Open Space Security از این به بعد از لیست محصولات کسپرسکی حذف می‌شود؟

بله حذف می‌شود ولی به این معنا نیست که کاربران فعلی این محصول دیگر نمی‌توانند از آن استفاده کنند. این حق طبیعی مشتریان است که بر روی محصول پیشین تا زمانی که آمادگی ارتقا به نسخه جدید را داشته باشند، همچنان خدمات پشتیبانی دریافت کنند.

آیا امکان جایگزینی این محصول با محصولات پیشین کسپرسکی از جمله Kaspersky Open Space Security برای کاربران پیشین کسپرسکی وجود دارد؟

بله این امکان وجود دارد. البته ارتقا به نسخه جدید در بسیاری از کشورهای جهان هزینه دارد اما کسپرسکی این امکان را فعلاً برای این مشتریان به صورت رایگان ارائه می‌کند و هر کدام از مشتریان که بخواهند از نسخه جدید استفاده کنند، می‌توانند آن را دریافت کنند. از سوی دیگر کسپرسکی کاربران را ملزم به استفاده از محصول جدید نمی‌کند و برای مدت محدودی، هم‌زمان با تحویل کالای جدید، مجوز استفاده از نسخه قدیمی نیز به مشتریان ارائه می‌شود تا اگر کاربری تمایل به استفاده از محصول قدیم را دارد به راحتی از آن استفاده کند.

راهکارهای جدید سازمانی شرکت کسپرسکی Kaspersky End Point Security for Business، نام دارد. وقتی شرکت کسپرسکی نام نقطه نهایی را برای این محصول امنیتی انتخاب کرده یعنی باید به تمام نیازهای امنیتی سازمان پاسخ داده شود، آیا این محصول چنین ویژگی دارد؟

قطعا همینطور است. کسپرسکی معتقد است که با توجه به افزایش تهدیدات اینترنتی و افزایش وابستگی افراد و سازمان‌ها به سیستم‌های کامپیوتری، امنیت یک سیستم صرفا محدود به آنتی ویروس نمی‌شود و طبیعتا عواملی همچون بهره‌وری کاربران، امنیت استفاده از تعاملات مالی اینترنتی، مدیریت و کنترل دسترسی به فایل‌ها، مدیریت و به‌روزرسانی سیستم عامل‌ها و بسیاری از امکانات مشابه دیگر تاثیر مستقیم و غیرمستقیم بر برقراری امنیت دارند و بنابراین یک محصول امنیتی جامع می‌بایست پاسخگوی تمامی این نیازها باشد که بدون شک محصول جدید کسپرسکی به نام KES4B، به خوبی به تمام این نیازها پاسخ داده است. به طور خاص با توجه به افزایش استفاده از موبایل‌های هوشمند و تبلت‌ها و تهدید بزرگی مانند گم شدن و دزدیده شدن این تجهیزات، این دستگاه‌ها توجه بسیاری از سازمان‌های امنیتی را به خود جلب کرده و برآورده کردن امنیت جامع در یک سازمان، بدون در نظر گرفتن امنیت آنها، به تکامل نمی‌رسد. کسپرسکی نیز برای این نیاز و سایر نیازهای امنیتی یک سازمان راه حل‌های جداگانه‌ای ارائه کرده است.

در معرفی این محصول جدید آن را «یک راهکار امنیتی جامع و فراگیری برای حفظ امنیت شبکه و اطلاعات سازمان‌ها» معرفی نموده‌اید و با بررسی مشخصات آن می‌بینیم که امکانات بسیاری بر روی آن قرار گرفته است. آیا بالا رفتن امکانات و وجود ابزارهای مختلف باعث پیچیده شدن این محصول نمی‌شود؟

نکته اول این که کسپرسکی دسته‌بندی امکانات محصول را به خوبی انجام داده است و در نتیجه امکانات روتین و اولیه، دم دست کاربر قرار گرفته است. نکته دوم این که مخاطبان ما در سازمان‌ها اصولا مدیران شبکه هستند که اطلاعات خوبی دارند و کاربران عادی نیستند. در واقع در این محصول، کاربر هیچ تنظیماتی را خود انجام نمی‌دهد و سیاست‌های اجرایی توسط مدیر شبکه اتخاذ و تنظیم شده و براساس دسته‌بندی‌های مختلف در کامپیوترها اعمال می‌شود. در واقع این امکانات کنترلی و مدیریتی، به صورت یکپارچه فعالیت می‌کنند. اما در مورد پیچیدگی امکانات برای مدیر شبکه، باید به این نکته اشاره شود که تلاش شده قسمت‌های کاملاً مجزایی برای هر امکان طراحی شود تا تداخل این امکانات یا تجمع همه این تنظیمات به صورت یکجا موجب سرگردانی مدیر شبکه نشود. به طور مثال امکان مدیریت

ابزارهـای قابل حمـل، کاملاً به طـور جداگانه ارائه می‌شـود و در نتیجـه ادمین با مراجعه به هر بخش دقیقـا می‌داند انتظارش از این بخش و تنظیمات آن چیسـت. به هر حـال نیازهای سـازمان‌ها (بـه ویژه سـازمان‌های متوسـط و بزرگ) به امکانات جدید افزایش یافته و برای تامیـن آن دو راه وجود دارد. یکی اسـتفاده از نرم‌افزارهـای گوناگون برای برطرف کردن هر نیاز و یکی استفاده از یک راهکار برای برطرف کردن تمام نیازهـا. البته طبیعتاً ما برای تمامی سـازمان‌هایی که مشـتری محصول ما هستند آموزش محصولات جدید را خواهیم داشت.

یکـی از مهم‌تریـن تفاوت‌های ایـن محصول با محصول پیشـین، اسـتفاده از Activation Code به جایLicense اعلام شـده اسـت. مزایای این روش جدید چیست؟

بسـیاری از سـازمان‌ها نگـران سوءاسـتفاده از لایسنس‌هایشـان هسـتند. Activation Code فضایـی را فراهم کرده که سـازمان‌ها می‌تواننـد به طور شـفاف بدانند چه تعدادی از مجوزهای خریداری شـده مورد اسـتفاده قرار گرفته و به ایـن ترتیب مدیریت بهتری روی چگونگی اسـتفاده از این مجوزها خواهند داشـت. حسـن قابل توجه دیگر این موضوع این است که پیش از این اگر سازمانی در طی مـدت اعتبار آنتی ویروس اقـدام به افزایش مجوزها می‌کرد، چاره‌ای نداشـت جز این که به تعداد جدید آنتی ویروس تهیه کرده و در نتیجه زمان پایان مجوز اسـتفاده سـازمان از آنتـی ویروس‌های قدیـم و جدیدش متفاوت می‌شـد. اکنـون این امـکان فراهم شـده که سـازمان به تعداد روزهای باقی مانده تا اتمام اولین مجوز خـود کدها را خریداری کند. در نتیجه مدیر شـبکه تنها لازم است به مدیریت یک کد بپردازد.

یکـی از نکاتی که هـم باعث گلـه کاربران کسپرسـکی شـده اسـت و هم در تست‌های مختلف باعث عقب ماندن کسپرسـکی بوده، کندشـدن کامپیوترها در صورت اسـتفاده از محصـولات این شـرکت بوده اسـت. آیا در نسخه جدید این ضعف برطرف شده است؟

تفاوت قابل توجه کسپرسکی با سایر محصولات موجـود در بـازار این اسـت که کسپرسـکی تنظیمـات امنیتی خود را در حالت پیش فرض، بـر روی تنظیمات حداقلی قـرار نداده و معتقد است تنظیمات پیش فرض باید به گونه‌ای باشد کـه کاربر بدون نیاز به تغییر تنظیمات، بهترین کیفیـت امنیت را بـر روی سیسـتم‌های خود تجربـه کند. بنابراین در نگاه اول ممکن اسـت نسخه کسپرسکی نسبت به سایر محصولات که در حالت پیش فرض برروی تنظیمات حداقلی تنظیم شده‌اند، کندتر به نظر بیاید.

با این حال گزارشات سازمان‌های معتبر سنجش آنتی ویروس‌ها نشـان می‌دهـد نتیجه عملکرد کسپرسـکی در مبـارزه بـا تهدیـدات امنیتی، نسـبت سایر رقبا همواره در بهترین حالت بوده اسـت. برای نمونه می‌توان بـه گزارش‌های دو نهاد معتبر AV TEST و AV comparatives اشـاره کنیم. از سوی دیگر اگر منابع مورد نیاز بر روی کامپیوتر جهت نصب آنتی‌ویروس‌های مختـلف را بـا یکدیگر مقایسـه کنیـد، متوجه می‌شـوید که منابع مورد نیاز نصب محصولات کسپرسـکی، همسان با سـایر آنتی‌ویروس‌ها و حتی در مواردی کمتر است که این موضوع نیز در تست‌های مختلف قابل مشاهده است.

در مقاله کوتاهی که در اختیار شما قرار داده‌ام به چند عامل کندی سیستم اشاره کرده‌ام. متاسفانه برخی کاربران بدون توجه به این نکات، کاهش سـرعت را به پای آنتی‌ویروس می‌نویسند. به هر حـال باید کاربـران به این موضـوع توجه کنند که تهدیدات امنیتی هر لحظه سیسـتم‌ها را تهدیـد می‌کنند و در نتیجه آنتی‌ویروس باید دائماً در حال کار باشـد و نمی‌توان از آن انتظار داشـت بر روی سـرعت عملکرد سیستم تاثیر نگذارد. دو سـه ثانیه تاخیر در عملکرد سیستم به حفظ امنیت اطلاعات می‌ارزد. به طور خاص در مورد KES4B، باید به این نکته اشـاره کنیم کـه امکانات این محصول افزایـش یافته اما به همان منابع و سخت‌افزار نسخه پیشین نیازمند اسـت. البته باز هم تاکید می‌کنم از نظر کارایی کسپرسـکی بهترین عملکرد را در تسـت‌های گوناگون کسب کرده است. ❖

کندی از آنتی‌ویروس نیست!

«همچنان که در مصاحبه با مدیرعامل شـرکت پارس آتنا دژ مطالعه نمودید، خانم بحری مقاله‌ای کوتـاه در اختیار ما قرار داده‌اند و در این مقاله به چند عامل کندی سیستم اشاره کرده‌اند.»

پیـش از اینکه آنتی‌ویـروس خـود را متهم به کند بـودن نمایید و کاهش سـرعت را به پای آنتی‌ویروس بنویسید، به این نکات توجه نمایید.

سخت افزار ضعیف

طبیعتاً اگر بر روی یک سیسـتم با سخت‌افزار ضعیـف که عملکرد پرسـرعتی نـدارد، آنتی ویـروس نصب کنیـم، نمی‌توانیـم انتظار عدم تغییر عملکرد بر روی سیستم را داشته باشیم. همچنین به طور مثال سیسـتم عامل ویندوز ۷ به تنهایی نیازمند دو گیگابایت رم اسـت و هر آنتی ویروسی نیز برای نصب شدن نیازمند یک گیگابایت فضای رم هست. در نتیجه نمی‌توان از سیسـتمی با دو گیگ رم و ویندوز ۷ انتظار داشـت پس از نصب آنتی ویـروس همچنان عملکرد پر سرعتی داشته باشد.

به‌روز بودن نرم‌افزارها

ممکـن اسـت آنتـی ویـروس ۲۰۱۰ فـرد به‌روزرسانی شده باشـد، اما طبیعتا این نسخه، از ورژن سال ۲۰۱۲ ضعیفتر عمل خواهد کرد؛ چرا که موتـور جسـت‌وجوگر و الگوریتم‌های شناسـایی مخاطرات، هر سـال تقویت شده و سرعت و عملکرد بهبود می‌یابد. از سوی دیگر سیسـتم عامل‌های قدیمی‌تـر دارای حفره‌های امنیتی بیشـتری هسـتند که در نتیجه احتمال آسیب‌پذیری سیستم را افزایش می‌دهند. آنتی ویروس نیز برای مقابله بـا این تهدیدات باید عملکرد بالاتری داشته باشد.

مرتب نگه داشتن هارد دیسک

حداقل بیسـت درصـد از فضای هـارد برای عملکـرد خـوب سیسـتم بایـد خالی باشـد. توصیه می‌شـود فایل‌های غیرضروری در هارد اکسـترنال نگهداری گردد تا از اسکن چندباره آنها توسط آنتی ویروس اجتناب شود.

راه دوم برای تمیز نگه داشـتن هارد، پاک کردن برنامه‌های غیرضروری اسـت. تعدد برنامه‌های غیرضروری سبب می‌شود این برنامه‌ها به دلیل این که در استارتاپ ویندوز فضایی را اشغال می‌کنند، هر بار، با روشن کردن کامپیوتر آغاز به کار کرده و در پشت زمینه سیستم همواره فعال باشند.

نکتـه دیگر این که نصـب و پاک کردن تعداد زیادی برنامه سبب می‌شود در بخش رجیستری تعداد زیادی «Registry Key» ایجاد شـود که این‌ها نیز در کندکردن سیستم موثر است. چرا که یکی از وظایف آنتی ویروس‌ها بررسـی مرتب فایل‌های رجیسـتری اسـت. به همین دلیل هم در بسـیاری مواقع مسـاله کند بودن سیستم پس از تعویض ویندوز برطرف می‌شود. به همین دلیل پیشـنهاد می‌کنیـم کاربران در کنار اسـتفاده از آنتی ویـروس از نرم‌افزارهای مدیریت و نگهداری سیسـتم عامل هم استفاده کنند تا نیاز به دفعات متعدد نصب نباشد.

یکپارچه سازی هارد (defragment)

هنگامـی که یـک نرم‌افزار را نصـب کرده یا فایلی را کپی می‌کنیم، ممکن اسـت با توجه به ظرفیت خالی، این نرم‌افزار چند تکه شده و در چند جای مختلف هارد نصب شـود. در نتیجه آنتی‌ویروس نیز ناچار اسـت برای بررسی یک فایل به چند جای هارد مراجعه کند. با استفاده از دستور یکپارچه‌سـازی، فایل‌ها و نرم‌افزارها در کنـار هم در هـارد قرار گرفته و سـرعت عملکرد آنتی ویروس بهبود می‌یابد. ❖

ضامن امنیت مکاتبات شما

معرفی امکانات امنیتی ایمیل سرور axigen

حسین رسولی
rasouly@ccwmagazine.com

اگر بازار ایمیل‌سرورها را بررسی کنیم، به نام axigen خواهیم رسید. axigen یکی از جدیدترین راه‌حل‌های پیغام رسانی است که با وجود عمر نسبتاً کم توانسته بسیار موفق عمل کند و هم اکنون نزدیک ۱۱ هزار سرور از امکانات این ایمیل سرور استفاده می‌کنند. با توجه به حضور موفق این برند در بازار ایران و به ویژه نفوذی که در سازمان‌های اداری داشته است، در ادامه نگاهی کوتاه داریم به امکانات امنیتی آن و قابلیت‌هایی که در حال حاضر در دسترس کاربران ایرانی قرار گرفته است.

در نگاه نخست سیستم پیکربندی برنامه به چشم می‌خورد که به شدت منعطف و قابل دستکاری است. تا نسخه پیش‌تر، سیستم این امکان را داشت که هر کار مورد نیاز مرسوم مدیر سیستم را انجام دهد. امکانات فیلترینگ و auto responder نیز از جمله قابلیت‌های چشم‌گیر دیگر این برنامه در نسخه‌های جدیدتر است.

Encryption

آکسیژن سرور از انواع Authenticution پشتیبانی می‌کند؛ این یعنی می‌شود طوری آن را برنامه ریزی کرد که فقط پیام‌ها و اتصالاتی را قبول کند که از طرف موجودیت‌های شناخته شده باشند. DIGEST-MD۵، GSSAPI، LOGIN، PLAIN و CRAM-MD۵ از جمله شیوه‌هایی هستند که برنامه در این راه از آنها مدد می‌گیرد.

SLL/TLS: پروتکل‌های ارتباطی آکسیژن امکان بهره‌وری از فناوری SSL/TLS را دارند. بدین طریق می‌توان پیام‌ها را به طور کدگذاری شده در شبکه دریافت و ارسال کرد و مانع سرقت یا دستکاری پیام‌ها در بین راه شد.

Multi-layer access control (firewall-like rules)

از جمله مهم‌ترین وظایفی که از یک میل سرور انتظار می‌رود، جلوگیری از حملات رد سرویس (DOS) و متوقف کردن اسپمرهاست؛ و هرچه این وظیفه سریع‌تر انجام می‌پذیرد، مطلوب‌تر است. از همین رو axigen در لایه اپلیکیشن خود (TCP Listener) مجهز به یک فایروال است که مدیران شبکه به لطف آن می توانند پارامترهای اتصال را کنترل و تنظیم نمایند.

Flow control (anti-bombing)

علاوه بر قوانین (rules) کنترل دسترسی، می‌توان محدودیت‌های کنترل هم در برنامه تعریف کرد تا مانع آوردلود استوریج و سرور شد. در ضمن از سرور در مقابل حملات Dos محافظت می‌شود.

SPF & DomainKeys compliant (check message sender & integrity)

آکسیژن دارای یک ماژول استاندارد SPF برای شناسایی و تایید ارسال کننده است - به شرطی که دامین راه دور به درستی با اطلاعات SPF پیکر بندی شده باشد.

Blacklist & Whitelist

می‌توان با axigen به طور دائم پیام‌های دریافتی از فرستنده‌های نامعتبر را ریجکت کرد. این لیست‌ها توسط مدیران سیستم (سطح سرور) قابل تعریفند و در ادامه کاربران نیز می‌توانند بنا به نیازهای شخصی خود (در سطح اینترفیس وب میل) تعاریف جدیدی بیفزایند. از طرف دیگر نیز ادمین‌ها می‌توانند لیست‌های سفیدی برای دریافت همیشگی ایمیل از منابع موثق و معتبر، چون شرکای تجاری یا شعب سازمان، تعریف و ایجاد کنند.

Country Filtering

ادمین‌ها می‌توانند با استفاده از دیتابیس IP - به - کشوری که دارند، کلیه ایمیل‌های رسیده از کشوری نامعتبر را بلوکه کنند یا برعکس، به طور خاص فقط ایمیل‌های رسیده از کشورهایی مشخص را اکسپت کنند.

AntiVirus Filtering (multiple applications)

بدنیست بدانید، در حال حاضر Axigen با ۱۵ برنامه آنتی ویروس معروف (مثل آویرا، کسپرسکی، بیت‌دفندر، مک آفی یا ترند میکرو) سازگار و تجمیع شده است.

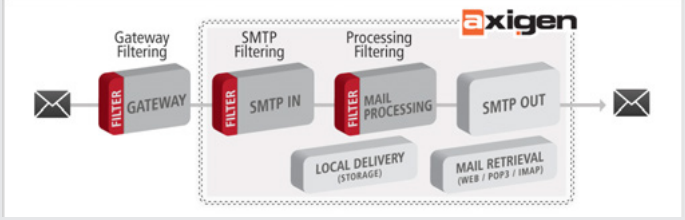
سیستم فیلترینگ پیشرفته این برنامه به مدیران سیستم اجازه می‌دهد مجموعه‌های مختلفی از فیلترها و اولویت‌ها را برای سطح کاربر، سرور یا دامنه تعریف نمایند.

مثلا بدین صورت:

دامین ۱: فیلتر با ۲ آنتی ویروس و یک برنامه آنتی اسپم

دامین ۲: فیلترینگ با فقط یک ضدویروس

General Manager: فیلتر با سه آنتی ویروس و یک آنتی اسپم



DNSBL

مدیران شبکه این امکان را خواهند داشت که IP یک تعداد از فرستندگان را با لیست‌های DNSBL(لیست سیاه DNS) تطبیق دهند تا ایمیل‌های خاصی را مسدود کنند و همزمان برای برخی رنج آی‌پی‌های مدنظرشان این حالت را استثنا کنند.

DNS Checks

با بررسی دامین مبدا مدخل‌های MX و IP مبدا یک مدخل DNS تبدیل شده، لیست‌های خاص‌تری ایجاد کرد و هرزنامه‌ها را رد نمود.

Message Acceptance Policies

همان طور که گفته شد، مدیران با تکیه بر دیتابیس IP-to-country که دارند، می‌توانند تمام ایمیل‌های رسیده از یک کشوررا ببندند یا فقط از کشورهای خاصی ایمیل قبول کنند .

Routing Policies

مسیر یابی مجازی: با نسبت دادن آی‌پی آدرس‌های خارجی مختلف به هر دامنه، IP های بلک لیست شده فقط بر دامین خودشان اثر می‌گذارند و دیگر دامین‌های فعال در همان سرور از گزند آنها در امان خواهند بود.

Anti-Impersonation

هر کاربر ملزم خواهد بود برای ارسال پیام، هویت خود را وارد و محرز کند. بدین روش از جعل هویت از طریق اکانت‌های محلی جلوگیری می‌شود.

جشنواره زمستانی گیت پروتکت

باخریدیکی از دستگاههای GPA250,GPO125, GPO75
۲۰% تخفیف برروی لایسنس خریداری شده دریافت نمایید.

باخریدهریک ازدستگاههای GPA400, GPA600, GPX800
GPX1000, GPZ2500, GPZ5000 دوره آموزشی رایگان
در کشور امارات (دبی)بگذرانید.

- تنها UTM دارای تکنولوژی eGUI برای مدیریت سریع و آسان
- برنده جایزه ۵ ستاره SC Magazine در سال 2012
- مدیریت کامل بر اساس شناسه کاربری (Layer 8)
- UTM مجاز دارای گواهینامه +EAL4 در سطح کشور
- با موتور ضد ویروس کسپرسکی

gateprotect®
www.gateprotect.com

به منظور همکاری و اخذ نمایندگی با ما در ارتباط باشید
partnership@tejarateamn.com
partnership@ictn.ir

با مراجعه به سایت و پاسخگویی به سوالات
برنده جوایز ارزنده شوید

فناوری تجارت امن
IT SECURITY SOLUTIONS
توزیع کننده انحصاری محصولات گیت پروتکت
در خاورمیانه , شمال آفریقا و هند
تلفن : ۳-۸۸۱۹۰۶۴۱(۹۸۲۱+)
www.tejarateamn.com

ICTN
IT solutions
توزیع کننده انحصاری محصولات گیت پروتکت درایران
تلفن : ۲۲۱۳۹۲۳۰ (۹۸۲۱+)
۳۳۷۹۷۰۰ (۹۸۴۱۱+)
www.ictn.ir

شرکت فناوری تجارت امن خاورمیانه

به دنبال برگزاری کارگاه آموزشی برای محصولات kaspersky،Gate Protect،GFI،Clavister

اقدام به برگزاری کارگاه های آموزشی تخصصی زیر نموده است:

رایانش ابری(Cloud Computing) ، IP نسخه ۶ (IPV6) ، امنیت برای مدیران ،
معماری امنیت ، مجازی سازی(Virtualization) ،
پایه های امنیت اطلاعات (پدافند غیرعامل) CSCU

C|SCU Certified Secure Computer User EC-Council

نماینده انحصاری برگزارکننده امتحانات تخصصی EC-COUNCIL

(یکی از معتبرترین مدارک تخصصیIT) در سراسر جهان

(CEH,CNSA,CSCU,CSSIP,CHFI,...)

EC-Council

همکاران فنی : موسسه کهکشان نور ،شرکت آینده نگاران (Ayco) ،شرکت ICTN ،شرکت دمسان رایانه، شرکت پارس ایمن افزار(Safe Soft)

gateprotect® KASPERSKY lab FIXME STICK STICK IT TO VIRUSES GFI acunetix WEB APPLICATION SECURITY clavister

فناوری تجارت امن IT SECURITY SOLUTIONS

تلفن دفتر تهران:
(+۹۸۲۱)۸۸۱۹۰۶۴۱-۳

با مراجعه به سایت و پاسخگویی به سوالات برنده جوایز ارزنده شوید

www.tejarateamn.com
info@tejarateamn.com

به منظور همکاری و اخذ نمایندگی با ما در ارتباط باشید
partnership@tejarateamn.com

برای ثبت نام وکسب اطلاعات بیشتربه وب سایت ما مراجعه وبا ما در تماس باشید

* برگزاری دوره های اختصاصی و گروهی برای کلیه سازمان ها و ارگان ها امکانپذیر می باشد

GFI MailEssentials®

- نرخ شناسایی هرزنامه بسیار بالا (بیش از ۹۹ %) از طریق استفاده از فناوری های ضد هرزنامه متنوع
- اسکن ویروس ها با موتورهای ضد ویروس چندگانه

GFI WebMonitor™

- بیشینه کردن استفاده از پهنای باند از طریق سهمیه زمانی / پهنای باند و نگهداری موقت صفحات و افزایش بهره وری با کنترل عادت وبگردی کارکنان
- جلوگیری از نشت اطلاعات از طریق وب سایتهای مهندسی اجتماعی(Social Engineering)

GFI

GFI LanGuard™

- نصب خودکار وصله های امنیتی محصولات مایکروسافت Macos و دیگر برنامه های کاربردی
- اجرای بیش از ۵۰۰۰۰ ارزیابی امنیتی در سراسر شبکه شامل کامپیوترها ، چاپگرها ، روترها ، سوئیچ ها و حتی محیط های مجازی

GFI EndPointSecurity™

- جلوگیری از سرقت / نشت اطلاعات به وسیله کنترل دسترسی به تجهیزات حافظه قابل حمل با کمترین زحمت
- جلوگیری از انتشار نرم افزارهای مخرب و غیر مجاز در شبکه

فناوری
تجارت امن
IT SECURITY SOLUTIONS
تلفن دفتر تهران:
۳-۸۸۱۹۰۶۴۱(۹۸۲۱+)

به منظور همکاری و اخذ نمایندگی با ما در ارتباط باشید
partnership@tejarateamn.com

توزیع کننده انحصاری محصولات جی اف آی در خاورمیانه , شمال آفریقا

با مراجعه به سایت و پاسخگویی به سوالات برنده جوایز ارزنده شوید
www.tejarateamn.com
info@tejarateamn.com

سال نو مبارک

arka

رایان سامانه آرکا

امنیت | مدیریت | پیام رسانی

AVIRA
axigen
ArkaGate NG
safetica
arkaVD
ARKAdesk
PaperCut
arkaBait
entensys
NetSupport
ManageEngine
fastvue
SPAM TITAN
PUTTER
CurrentWare
GFI

رایان سامانه آرکا – امنیت | مدیریت | پیام رسانی
نشانی جدید: تهران، خیابان شهید بهشتی، خیابان پاکستان، کوچه چهارم، پلاک ۱۱ ، واحد ۷
تلفن : ۸۸۱۷۲۹۰۹ (۰۲۱)
فکس : ۸۸۱۹۱۳۲۴(۰۲۱)
www.arka.ir | info@arka.ir