

برای حضور در بازار داخلی فرصت می‌خواهیم

می‌گرد بررسی توانمندی‌های داخلی
در مقابله با تهدیدات سایبری

■ آنتی ویروس‌های خارجی پالایش می‌شوند

■ هر روز ۷۰ هزار حمله سایبری

■ فرهنگ سازی در فضای سایبر

■ جاسوس چند چهره



محمود محسنی نیا



کاتم قسبی



عاصم تحقیقان



حمیدرضا سعدی



علیرضا صالحی

+010110101101010110101011010101101

+010110101101010110101011010101101

+ + +

+ + +

+010110101101010110101011010101101

010110101101010110101011010101101

اولین تولید کننده ضد ویروس در ایران

۱۸ سال سابقه

نرم افزار ضد ویروس
ایمن



نسخه تک کاربره ققنوس با نصب آزمایشی ۲ ماهه رایگان
نسخه شبکه ققنوس با نصب آزمایشی ۱ ماهه رایگان



تلفن: ۶۶۹۰۰۶۱۱-۱۶
نمابر: ۶۶۹۰۰۶۱۷

تهران - خیابان جمهوری اسلامی - بین جمالزاده و کارگر - شماره ۱۱۱۷ - طبقه سوم و چهارم
www.lmenAntiVirus.com

شرکت مهندسی مهران رایانه
Mehran Rayaneh Co.

info@lmenAntiVirus.com

رئیس کمیسیون افتای سازمان نظام صنفی رایانه‌ای خبر داد

آنتی‌ویروس‌های خارجی پالایش می‌شوند

عضو هیئت‌مدیره سازمان نظام صنفی رایانه‌ای استان تهران تأکید کرد: در این مرحله بازار هدف صرفاً سازمان‌های دولتی قرار داده شده که باید ضد بدافزارهای خود را از لیست اعلامی و مورد تایید سازمان فناوری اطلاعات انتخاب نمایند.

وی ادامه داد: علاوه بر این، شناسایی و تعیین ملاک‌های ارزیابی شرکت‌های عرضه‌کننده این محصولات نیز جزو دستور کار این کارگروه است. در این راستا هم‌اکنون کارگروه ساماندهی ضدبدافزارهای خارجی در کمیسیون افتای سازمان نظام صنفی رایانه‌ای استان تهران، فراخوانی را برای شناسایی شرکت‌های ارائه‌دهنده ضد بدافزارهای خارجی اعلام کرده است.

وی ادامه داد: در این فراخوان شرکت‌های واردکننده و فروشنده ضدبدافزارهای خارجی که با سازمان‌های دولتی همکاری دارند، باید اطلاعات خود را به صورت خوداظهاری به ثبت برسانند.

وی ادامه داد: با تشکیل بانک اطلاعاتی شرکت‌ها و برندهای واردکننده ضدبدافزارهای خارجی، ارگان‌های دولتی با مراجعه به آن قادر خواهند بود مطابق با نیاز سازمانی‌شان نرم‌افزار و خدمات امنیتی را از شرکت‌هایی که اسامی آنها در این بانک اطلاعاتی ذکر شده و صلاحیت‌شان به تایید رسیده سفارش دهند.

آریا گفت: در مرحله بعد نیز اطلاعات خوداظهاری شرکت‌ها با واقعیت تطبیق داده خواهد شد.

این عضو هیئت‌مدیره سازمان نظام صنفی رایانه‌ای استان تهران خاطر نشان کرد: در فاز نخست محدوده این فراخوان، استان تهران است و تنها ارائه‌دهندگان نسخه‌های شرکتی و شبکه‌ای ضد بد افزار، مورد بررسی قرار می‌گیرند و فراخوان نیز روی سایت سازمان نظام صنفی رایانه‌ای استان تهران به آدرس Tehran.irannsr.org قابل دسترس است.

رئیس کمیسیون افتا سازمان نظام صنفی رایانه‌ای تهران گفت: با اعلام ممنوعیت ورود ضدبدافزارهای خارجی، قرار شد به موازات حمایت از تولید ضدبدافزارهای بومی از برخی آنتی‌ویروس‌های خارجی برای تأمین امنیت استفاده شود.

به‌نظر آریا اظهار داشت: پس از اعلام ممنوعیت ورود ضدبدافزارهای خارجی به کشور از سوی وزیر ارتباطات و فناوری اطلاعات، باید راه‌حل جایگزینی برای این موضوع پیدا می‌شد.

رئیس کمیسیون افتای سازمان نظام صنفی رایانه‌ای استان تهران افزود: با اعلام این ممنوعیت، علاوه بر ایجاد اختلال در تجارت شرکت‌های واردکننده ضد بدافزار، موضوع مهم‌تر مطرح شده، تأمین امنیت مطلوب بود.

عضو هیئت‌مدیره سازمان نظام صنفی رایانه‌ای استان تهران گفت: در این زمینه طی جلساتی با معاون گسترش سازمان فناوری اطلاعات، قرار شد برای راه‌حل میان‌مدت، در مرحله نخست از برخی آنتی‌ویروس‌های خارجی برای تأمین امنیت استفاده شود و به موازات آن تولید و استفاده از ضدبدافزارهای تولید داخل نیز حمایت و پیگیری گردد.

آریا گفت: از این رو با همکاری مشترک سازمان فناوری اطلاعات ایران و کمیسیون افتای سازمان نظام صنفی رایانه‌ای استان تهران، "کارگروه ساماندهی ضد بدافزارهای خارجی" تشکیل شد که جلسات آن با حضور نمایندگان هر دو سازمان به صورت مرتب تشکیل می‌شود.

وی ادامه داد: در این کارگروه، ملاک‌های ارزیابی ضد بدافزارهای خارجی مشخص و سپس به سازمان فناوری اطلاعات ایران ارسال می‌شوند. سازمان فناوری اطلاعات با لحاظ کردن ملاحظات حاکمیتی و ملی، ضد بدافزارهای اعلام‌شده را مورد ارزیابی قرار می‌دهد و در نهایت ضدبدافزارهای مورد تایید اعلام می‌شوند.

معاون وزیر ارتباطات و فناوری اطلاعات از انجام روزانه ۷۰ تا ۷۳ هزار حمله سایبری در دنیا خبر داد.

علی حکیم‌جوادی درباره‌ی حملات سایبری اظهار کرد: اکنون هیچ کشوری در دنیا وجود ندارد که بگوید تاکنون با حملات سایبری مواجه نشده است، چراکه در حال حاضر از یک هکر آماتور تا هکرهای سازمان یافته و گاه دولت‌ها هم می‌توانند مزاحمت‌هایی برای سایر کاربران ایجاد کرده و حتی به زیرساخت‌های حیاتی کشورها حمله کنند.

رئیس سازمان فناوری اطلاعات در عین حال عنوان کرد: طبق برخی آمارهای موجود، روزانه بیش از ۷۰ تا ۷۳ هزار حمله مختلف سایبری صورت می‌گیرد و در چنین شرایطی باید سازوکاری مناسب برای مقابله با این ویروس‌ها و بدافزارها وجود داشته باشد.

حکیم‌جوادی در ادامه راه‌اندازی مرکز "ماهر" را اقدامی در همین راستا دانست و خاطر نشان کرد: نباید تعداد حملات به چند حمله محدود خلاصه شود، اما با این حال تفاوت‌های عمده‌ای بین حمله‌های صورت گرفته وجود دارد و این حمله‌ها گاه به گونه‌ای بوده است که نمی‌توان آن را از طریق یک فرد ارزیابی کرد، چراکه سرمایه‌گذاری‌های بسیاری برای آن‌ها صورت گرفته است.

رئیس سازمان فن‌آوری اطلاعات در ادامه با تاکید بر این‌که تاکنون با تحقیقات و تلاش‌های صورت گرفته کارشناسان موفق به شناسایی سریع ویروس‌ها و بدافزارهای مهاجم شده‌اند، گفت: یکی از راهکارهایی که می‌توان برای جلوگیری از گسترش این موضوع مورد استفاده قرار داد، آن است که بخش‌های دولتی و حتی خصوصی ارتباط خوبی با مرکز ماهر داشته باشند.

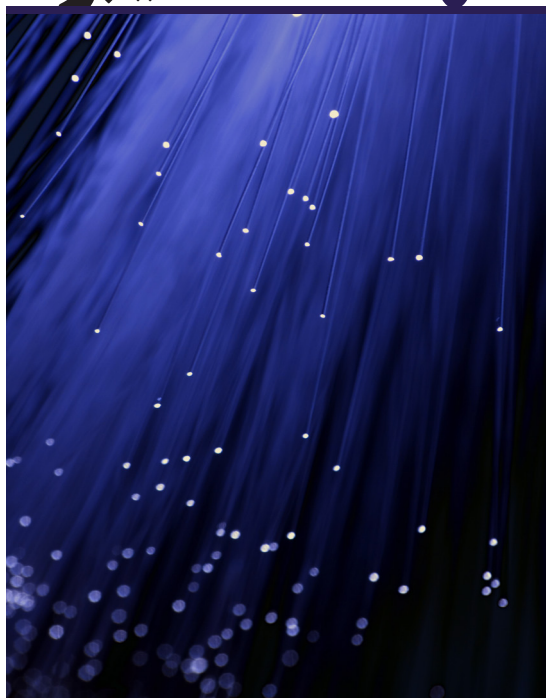
وی در ادامه با تاکید مجدد بر این‌که بحث حملات سایبری مختص به یک کشور نمی‌شود، یادآور شد: در اجلاس WSIS نیز بسیاری از کشورها این مساله را یکی از تهدیدهای خود عنوان کردند و حتی برخی کشورها آنقدر بر روی این موضوع حساسیت نشان دادند که این حملات را در حد نظامی ارزیابی کردند.

او ادامه داد: خوشبختانه اکنون همکاری‌های خوبی بین فعالان حوزه‌ی سایبر صورت گرفته و ما امیدواریم با همکاری‌های بیشتر دست‌اندرکاران پاسخ به‌موقعی برای این تهدیدها داشته باشیم.

حکیم‌جوادی در عین حال راه‌اندازی شبکه ملی اطلاعات و دسترسی بخش‌های اجرایی به شبکه‌ای برون‌مرزی را یکی از راهکارهای مهم کاهش این خطر برشمرد.

معاون وزیر ICT خبر داد:

هر روز هزار حمله سایبری



عامل پیشگیری از وقوع جرم:

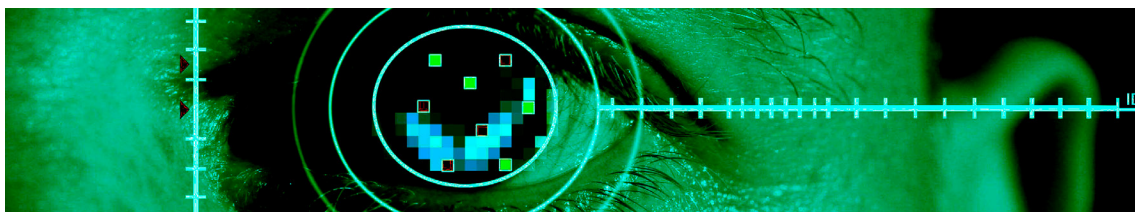
فرهنگ سازی در فضای سایبر

رئیس پلیس فتا در ادامه به علل و عوامل بسیاری در شکل گیری از جرایم از جمله عوامل اقتصادی فرهنگی، مشکلات روحی روانی، تلقین افسردگی، عصبانیت، حسادت، انتقام جویی، حس تنفر، تفریح و سرگرمی، خودکم بینی، حقارت، حس رقابت و کنجکاوی اشاره کرد.

این مقام مسئول در خاتمه از ویژگی های منحصر به فردی که فضای سایبری را از دیگر رسانهها متمایز می سازد، جهانی بودن آن و شکسته شدن مرزهای جغرافیایی برشمرد، تصریح کرد: ارتقای سطح اطلاعات نسبت به فضای مجازی و اطلاع رسانی در زمینه جرایم سایبری و راه های مقابله با آن، ارتقاء سطح باورهای دینی و اخلاقی خصوصا در بین جوانان و نوجوانان نمونه های پیشگیری از شکل گیری جرایم در فضای مجازی است.

رئیس پلیس فتا با اشاره به اینکه فرهنگ سازی استفاده از فضای سایبری عامل پیشگیری از وقوع جرایم می باشد، خبر داد: چشم انداز پلیس فتا در عرصه کنترل جرایم کشف ۸۰ درصدی است.

سردار هادیانفر رئیس پلیس فتا با اشاره به اینکه ابزار فن آوری اطلاعات نقش انکار ناپذیری در رقابت های سیاسی، امنیتی، اقتصادی، تجارت، اخلاق و دینی در عرصه های ملی و بین المللی ایفا میکند، گفت: اهداف پلیس فتا ناجا حفاظت از اموال، منافع و اسرار ملی و ارتقاء امنیت و حفظ حریم خصوصی افراد در فضای سایبر در حوزه وظایف ناجا می باشد. وی در ادامه از افزایش ۶۰ درصدی قدرت پلیس در فضای سایبری خبر داد و اظهار داشت: چشم انداز پلیس فتا در عرصه کنترل جرایم کشف ۸۰ درصدی است.



معاون وزیر ICT خبر داد:

دستور رئیس جمهوری برای استخدام نیرو در حوزه امنیت اطلاعات

این شکل جذب شوند، توضیح داد: محدودیتی برای جذب نیرو در این زمینه تعیین نشده و تنها گفته شده است که نیروهای مورد نیاز تامین شوند.

حکیم جوادی در بخش دیگری از صحبت های خود هم به ارائه الکترونیکی خدمات دولتی اشاره کرد و گفت: قرار بود تا پایان سال ۹۱ تمام بخش های اجرایی به شبکه ی ملی اطلاعات متصل شوند که با دستور رئیس جمهوری قرار بر آن شد که در این موضوع تسریع شود و تا دو ماه دیگر تمام دستگاه ها به این شبکه متصل شوند.

معاون وزیر ارتباطات و فناوری اطلاعات از دستور رئیس جمهوری برای جذب نیروهای انسانی در زمینه ی امنیت فن آوری اطلاعات خبر داد.

علی حکیم جوادی، رئیس سازمان فن آوری اطلاعات، گفت: مدتی است برای تامین امنیت بیشتر، رئیس جمهور دستور جذب نیروهای انسانی مورد نیاز در زمینه ی امنیت فن آوری اطلاعات را صادر کرده و قرار است این نیروها از طریق معاونت توسعه نیروهای ریاست جمهوری تامین شود که به نظرم این موضوع خبر خوبی است. معاون وزیر ICT در پاسخ به این سوال که قرار است چه تعداد نیرو به

می‌توان ویروس شعله را در میان بدافزارها و جاسوس‌افزارها یکی از خطرناک‌ترین و مخرب‌ترین نوع بدافزار دانست، در یک نگاه می‌توان مدعی بود که این ویروس بسیار پیشرفته‌تر از Stuxnet و DuQu است، ساختار ماژولار و انعطاف پذیر و بسیار پیچیده و رمزگذاری شده به گونه‌ایست که امکان دیباگ و مهندسی معکوس کردن را بسیار دشوار و یا حتی غیرممکن می‌سازد، این ویروس ظاهراً هر اقدامی را برای مهاجمان فراهم می‌سازد.

جمع آوری اطلاعات و فرستادن آنها، نفوذ در شبکه‌های بزرگ (گاه صنعتی و مهم)، از بین بردن اطلاعات سیستم آلوده، قدرت جست‌وجو، تحلیل و پردازش گونه‌های خاص از فایل‌ها، از کار انداختن آنتی‌ویروس‌ها، امکان ارتباط و ارسال گزارش با مرکز فرماندهی خود و ... اینها تنها بخشی از قابلیت‌های ویروس شعله است.

در این گزارش بیشتر مواردی را مورد بررسی قرار می‌دهیم که از دید کثیری از تحلیلگران پنهان مانده است.

با بررسی ویروس شعله میتوان بیان کرد که این ویروس از طریق فلش دیسک انتشار پیدا می‌کند و همچنین قابلیت منتشر شدن در سطح شبکه را نیز داراست، ویروس شعله برای آلوده ساختن از قابلیت Autorun ویندوز بهره می‌برد.

نکته جالب توجه در بررسی ویروس شعله این بود که این بدافزار برای بدست آوردن اطلاعات در مورد قابلیت‌های پهنای باند در فهرست وب سایت‌های خود از سه وب سایت ایرانی استفاده کرده است، که تاکید بر آن دارد، ایران یکی از اهداف اصلی ویروس شعله بوده است.

از سایر ویژگی‌های ویروس شعله میتوان به سوء استفاده از حفره‌های امنیتی، سرقت کلمات رمز و عبور، متوقف کردن پروسه‌های امنیتی، شناسایی و از کار انداختن بیش از ۱۰۰ نرم‌افزار آنتی‌ویروس، ضد بدافزار، فایروال و ... ، قابلیت اجرا در Windows XP, Vista, 7, پردازش و تحلیل فایل‌هایی با پسوندهای

doc, *.docx, *.xls, *.dwg, *.kml *.ppt, *.csv, *.txt, *.vsd, *.ora, *.eml, *.url, *.pub, *.rdp, *.ssh, *.ssh2 تصویربرداری از صفحه نمایشگر، ضبط صدا و استفاده از آنها برای مقاصد جاسوسی اشاره کرد. این ویروس توانایی از بین بردن خود را نیز دارد.

لازم به ذکر است که قریب به ۹۰٪ اطلاعاتی که در محافل خبری معتبر و رسمی در مورد ویروس شعله ارائه شده درست بوده و مورد تأیید آزمایشگاه ضد بدافزار ایمن می‌باشد. گرچه برای پی بردن به تمامی اصرار نهفته در این بدافزار نیاز به زمانی به مراتب بیشتر از اینهاست. آزمایشگاه ضد بدافزار ایمن این افتخار را دارد که تا کنون دو گونه متفاوت از ویروس شعله را شناسایی و ضد بدافزار خود را بروز نموده است.

در پایان لازم است به این نکته اشاره شود که استاکس نت، شعله و ... آخرین تهدیدات و حملات سایبری دشمنان این خاک نخواهند بود، به امید مقابله با چنین تهدیداتی قبل از وقوع اتفاق.

تحلیل آزمایشگاه ضد بدافزار ایمن از بدافزار فلیم

جاسوس چند چهره

بعد از حمله سایبری به شرکت نفت آزمایشگاه ضد بدافزار ایمن که نخستین آزمایشگاه ضد بدافزار ایرانی می‌باشد خود را موظف دانست تا همانند حملاتی همچون استاکس نت باز به دنبال راه‌های شناخت و مقابله با این بدافزار باشد.

میزگرد بررسی توانمندی‌های داخلی در مقابله با تهدیدات سایبری

برای حضور در بازار داخلی فرصت می‌خواهیم

شاید در سال ۱۹۸۹ که اولین حمله سایبری به سیستم کامپیوتری سازمان فضایی آمریکا (ناسا) به عنوان ابزار قدرت و نفوذ به کشورها و سرقت اطلاعات آن‌ها انجام شد، کمتر کسی فکر می‌کرد، بدافزارها و ویروس‌های جاسوس روزی بتوانند بدون هیچ جنگ و خونریزی به عنوان یکی از بزرگترین و قدرتمندترین روش‌های حمله به کشورها تلقی شوند. طی سال‌های اخیر و به‌ویژه با گسترش فعالیت‌های هسته‌ای ایران، یکی از کانون‌های اصلی و همچنین مرکز توجه نفوذگران، ایران و فعالیت‌های هسته‌ای آن بوده است. به‌طوریکه از دو سال قبل تاکنون، تهدیدات سایبری گسترده و البته هدفمندی تحت عنوان استاکس‌نت، دوکو و بعدتر از آن فلیم، با هدف سرقت اطلاعات و ضربه زدن به زیرساخت‌های صنعتی ایران طراحی شد. از این رو بیش از هر زمان دیگری سازمان‌ها و شرکت‌های داخلی به فکر تامین امنیت شبکه‌ها در مقابله با این تهدیدات افتادند و در این راه به عنوان اولین قدم اقدام به خریداری تجهیزات امنیتی نمودند.

با واردات گسترده تجهیزات امنیتی به کشور، حال این سوال مطرح می‌شود که آیا در وضعیت جدید و همچنین با وجود تولیدکنندگان داخلی که سعی در بومی‌سازی تجهیزات امنیتی دارند، آیا باز هم سازمان‌های بزرگ برای تامین امنیت و حفظ اطلاعات خود و مقابله با تهدیدات سایبری، باید به تجهیزات امنیتی خارجی تکیه کنند؟

در راستای برگزاری سلسله میزگردهای تخصصی، افتانا برای پاسخ به این سوالات، این‌بار بررسی توانمندی‌های بخش خصوصی و تولیدات داخلی در مقابله با تهدیدات سایبری را موضوع میزگرد جدیدی قرار داده است. مهندس عامر نجفیان‌پور (رئیس هیئت مدیره گروه داده پردازان دوران)، مهندس حمیدرضا سعدی (عضو هیئت مدیره شرکت مهران رایانه)، مهندس محمود محسنی‌نیا (معاون اجرایی شرکت امن‌افزار گستر شریف) و مهندس کاظم قنبری (مدیر عامل شرکت قاصدک سامانه) و مهندس علیرضا صالحی (دبیر کمیسیون افتای سازمان نظام صنفی تهران) حاضران در این میزگرد بودند. مشروح این گفت و گور را بخوانید.

امنیتی مشکل را سر بسته مطرح کرده و می ترسند اطلاعاتی در اختیار ما قرار دهند!

محسنی نیا: بحث ویروس ها و بد افزار های جاسوسی نظیر استاکس نت و فلیم تمام شدنی نیست و نه تنها برای ایران بلکه در کل دنیا اتفاق می افتد. به نظر من باید در این جلسه به دنبال راهکارهایی باشیم تا اجازه ندهیم، بیشتر از این به ما صدمه بزنند.

قنبری: به نظر من بزرگترین ویروس که تاکنون باعث خروج اطلاعات از سازمان شده و به عنوان یک تهدید مهم شناخته می شود، ویروس دوپا یا همان نیروی انسانی شاغل در سازمانها است.

یک تیم تخصصی پشت ویروس فلیم

نجفیان: من موافقم در مورد راهکارها صحبت کنیم اما این نکته را هم نباید فراموش کنیم، همین حالا هم خیلی از شرکتها راهکار دارند، اما شاید راهکار جامع و کاملی نباشد. استفاده از ضد ویروس و فایروال و ایجاد شبکه های امنیتی یک لایه و دو لایه از راهکارهای سازمانها برای مقابله با نفوذ است اما اینکه چرا فلیم توانست اینقدر خوب نفوذ پیدا کند، موضوع مهمی است. تقریباً همه تأیید می کنند ویروس فلیم، یکی از قوی ترین ویروس هایی بوده که تاکنون نوشته شده است. به نظر من تیمی که این ویروس را نوشته، یک تیم ویروس نویس صرف نبوده بلکه هر بخش آن توسط تیمی متخصص نوشته شده است.

ویروس فلیم برای ورود به سیستم، الگوریتم MD5 ویندوز را هک می کند. چند سال قبل متخصصان قابل نفوذ بودن MD5 را به مایکروسافت تذکر دادند. مایکروسافت هم این امکان را از همه بخش های ویندوز به جز بخش Auto Update حذف کرد. ویروس فلیم هم دقیقاً از همین نقطه، سوءاستفاده کرد. این ویروس روی بخش Auto update ویندوز نشسته و اصلاحیه های مایکروسافت را می گیرد. خودش هم چند فایل دیگر به آن اضافه می کند.

از آنجائیکه فایل های اضافی در کنار اصلاحیه های مایکروسافت امضا می شوند، هیچ ضد ویروسی نمی تواند فایل های مخرب را از سایر فایل ها تشخیص دهد. کاربران همه فایل ها را نصب می کنند، بی خبر از اینکه فایل های مخرب هم بین آنها وجود دارد. با این توضیح می خواهیم به این نتیجه برسیم که این تکنیکها فراتر از یک ویروس نویسی ساده است.

قنبری: قطعاً دانش ویروس ها و ویروس نویسی ها به مرور زمان بیشتر شده است اما مشکلی که به ویژه در سازمان های دولتی با آن روبرو هستیم این است که برای نفوذ به شبکه این سازمانها نیازی به این همه پیچیدگی

قنبری: بزرگترین ویروس که تاکنون باعث خروج اطلاعات از سازمان شده و به عنوان یک تهدید مهم شناخته می شود، ویروس دوپا یا همان نیروی انسانی شاغل در سازمانها است.

صالحی: دو سال قبل ویروس به نام استاکس نت به عنوان یکی از جدی ترین تهدیدات سایبری وارد کشور شد. حالا بعد از گذشت زمان، شاهد تهدیدات جدیدتری چون ویروس فلیم هستیم. در میزگرد امروز می خواهیم به بررسی توان تولیدکنندگان داخلی در مقابله با تهدیدات سایبری بپردازیم. متأسفانه یکی از مهمترین دغدغه های مدیران شرکتهای بخش خصوصی صرف نظر از راهکارهای داخلی یا خارجی برای مقابله با تهدیدات، عدم همکاری بخش دولتی در این زمینه است. برای شروع لطفاً هر یک از مدیران که در این زمینه تجربه ای دارند بفرمایند.

سعیدی: متأسفانه ویژگی ویروسها این است که خیلی زودتر از اینکه از وجودشان خبردار شویم، به شبکه ما نفوذ کرده و عملیات تخریبی را انجام داده و بعد از اینکه تأثیر مخرب شان بر شبکه ما وارد شد، شناسایی و تحلیل می شوند. مثلاً در مورد ویروس استاکس نت، کارشناسان پس از گذشت یکسال که آسیب های زیادی به شبکه ها وارد شده بود، پی به وجود این ویروس برده و پس از دو ماه شروع به تحلیل عملکرد آن کردند. در مورد ویروس فلیم هم همین اتفاق افتاد.

اما در توضیح اینکه چرا معمولاً ویروسها اینقدر دیر شناسایی می شوند، سرورهای داخلی ما روزانه بین ۴۰ تا ۵۰ هزار بد افزار را جمع آوری می کنند که بین آنها هم چندین جاسوس افزار هم وجود داشته باشد. اما اینکه کدامیک از اینها ارزش تحلیل و بررسی را دارند، مثل گشتن به دنبال یک سکه در انبار سیلو است و عملاً امکان پذیر نیست. با اینکه ویروس فلیم بهمن ماه شناسایی شد اما تحلیل و بررسی عملکرد آن از دو هفته قبل (واسط تیرماه) انجام شد.

رسالت آزمایشگاه مهران رایانه این است که وقتی وجود ویروس به طور جدی مطرح شد، در آرشیو آزمایشگاه آن را جستجو کرده و در نهایت اقدام به تحلیل آن می کند اما به دلیل اینکه این کار هیچ ارزش افزوده ای برای ما ندارد و همچنین متولی دستگاه های دولتی در بحث اطلاع رسانی نیستیم، عجله ای هم برای انتشار اطلاعات حاصل از تحلیل ویروسها نداریم!

صالحی: برخورد سازمانها در زمان کشف ویروس چگونه است؟ آیا برخورد حساسی است؟ آیا به کارشناسان شما برای بررسی و نمونه برداری اجازه ورود به سازمان داده می شود؟

سعیدی: دقیقاً مشکل ما در آزمایشگاه همین است. به دلیل رسالت آزمایشگاه مهران رایانه، هر سازمانی بعد از بروز مشکل با ما تماس می گیرد. اما متأسفانه نه برای تحلیل ویروس هزینه ای پرداخت می کنند و نه تمایلی به رسانه های شدن موضوع دارند.

قنبری: در سایر کشورها با یک روال مشخصی مثلاً داشتن امضا و یا نشانه، کارشناسان مرتبط حق ورود به سازمان و نمونه برداری دارند. اما در کشور ما اگر در سازمان اطلاعاتی هم در مورد ویروس وجود داشته باشد، به دلایل



کاظم قنبری

محسنی‌نیا: خرید تجهیزات امنیتی به معنی افزایش امنیت نیست و حتی ممکن است باعث نا امنی بیشتر هم بشود.

تامین امنیت به فکر خرید تکنولوژی می افتند و با خریدن یک فایروال می خواهند امنیت همه جانبه‌ای برقرار کنند! سازمان‌ها بعد از برقراری کلیه این جوانب، باید به دنبال پیاده‌سازی یک راه‌حل امنیتی هم باشند. مدتی است محثی تحت عنوان SOC در بعضی سازمان‌ها مطرح می شود. SOC مرکز عملیات امنیت به عنوان چتری بر روی همه راه حل‌های امنیتی قرار می گیرد.

با اینکه هیچ زمانی هیچ ضدویروسی قادر به شناسایی کل ویروس‌ها نخواهد بود، اما از طریق شواهد و همچنین ابزارهای مختلف می توان پی به وقوع یک اتفاق مشکوک برد. ویروس‌های رایانه‌ای هم مثل ویروس سرماخوردگی به مرور بیشتر شده و کهنه می‌شوند. هر قدر سازمان دیرتر متوجه حضور و فعالیت آن‌ها شود، جلوگیری از گسترش اثرات مخرب آنها هم سخت‌تر خواهد شد. بی توجهی به اتفاقات کوچک و جزئی باعث می شود، ویروس تا جایی گسترش پیدا کند که قطع شبکه و اینترنت تنها راه حل باقی‌مانده می‌شود.

اما چه کار می‌توان کرد تا خیلی زودتر متوجه فعالیت‌های مخرب شد؟ ابزارهایی وجود دارند که کلیه گزارش‌های شبکه را در جایی متمرکز، جمع‌آوری می‌کنند. هر کدام از این ابزارها به نوبه خود خبر از اتفاق کوچکی از آن اتفاق اصلی و بزرگ را گزارش می‌کنند. با کنار هم قرار دادن این اطلاعات، می‌توان از وقوع یک اتفاق غیرعادی باخبر شد. این اقدامات حتماً باعث خواهد شد سازمان‌ها نسبت به وجود ویروس، خیلی زودتر واکنش نشان داده و اقدامات لازم، برای مقابله با آن نیز انجام شود.

صالحی: خیلی از سازمان‌های دولتی این اتفاقات را ثبت می‌کنند اما متأسفانه در اغلب موارد این اطلاعات بدون تحلیل و بررسی رها می‌شوند.

سعیدی: به نظر من یک ویروس گنجی از اطلاعات فنی است که هنوز کسی متوجه آن نشده است. در واقع ویروس‌ها فرصت‌های مناسبی برای شرکت‌های خصوصی هستند تا نسبت به بروز کردن اطلاعات خود اقدام کنند. البته شرکت‌های خارجی در این زمینه بسیار فعال عمل کرده‌اند اما سازمان‌های ما در مواجهه با این شرایط، حالت تدافعی به خود می‌گیرند. در امریکا هم‌زمان با همایش کلاه سیاه‌ها، مسئولان امنیت اطلاعات سازمان‌ها هم حضور دارند و سعی می‌کنند از توانمندی‌های ویروس نویسان بهره‌برند. اما در ایران سازمان‌ها از بررسی وضعیت و قابلیت نفوذ سازمانشان واهمه دارند. به نظر من بخش خصوصی باید برای به چالش کشیدن این وضعیت وارد عمل شود و نمره منفی را به سازمانی بدهد که برای جلوگیری از نفوذ، شبکه دو تکه طراحی کرده و کلا شبکه داخلی اش قطع است!

صالحی: متأسفانه خیلی از سازمان‌ها اعتقاد دارند که تنها راه حل جلوگیری از نفوذ، داشتن یک شبکه دو تکه است.



محمود محسنی‌نیا

نیست. ویروس‌های خیلی ساده‌تر از ویروس فلیم، منجر به خروج انبوهی از اطلاعات از سازمان‌ها می‌شود. گهگاه در سازمان‌ها دیده‌ایم پس از نصب یک برنامه، رمز عبور آن را ۱ تا ۶ گذاشته‌اند. به نظر من در شرایط فعلی شاید تکنولوژی پشت این ویروس‌ها آنقدر مهم نباشد. بلکه روندی که باید در سازمان‌ها تعریف شود تا اساساً نفوذ را غیرممکن کند، مهم‌تر است. به نظر من قبل از هر چیز باید فرهنگ سازمان‌های ما در حفظ امنیت اطلاعات سازمانی تغییر کند. اینکه بدانند حمله چیست؟ چه اقدامات پیشگیرانه‌ای وجود دارد و حتی بعد از بروز حمله چه باید کرد.

در حالیکه رویکرد فعلی سازمان‌ها در مواقع این چنینی، عدم اطلاع رسانی و همچنین جلوگیری از ورود کارشناسان به داخل سازمان است. من در دفتر رئیس یکی از بانک‌ها بودم و رئیس بانک به من گفت همین حالا که شما در دفتر من هستید، یعنی بانک ما امن نیست. باید چنین دیدگاهی تغییر کند.

سازمان‌های ما در حالی فقط به دنبال خرید سخت افزارهای امنیتی هستند که هنوز فرهنگ استفاده از آنها را ندارند. بسیار اتفاق افتاده ما به سازمانی سخت افزار فروختیم اما هنوز برای دریافت رمز عبورش با ما تماس نگرفته‌اند این یعنی که آن سخت‌افزار در سازمان بلا استفاده مانده است.

محسنی‌نیا: بله چند وقتی است، موجی از خرید سخت افزارهای امنیتی بین شرکت‌ها شکل گرفته و همه به فکر افزایش تجهیزات امنیتی خود هستند. اما خرید تجهیزات امنیتی به معنی افزایش امنیت نیست و حتی ممکن است باعث ناامنی بیشتر هم بشود. مهم مدیریت بحران از طریق فرایندهای تعریف شده است! حمله سایبری در همه جای دنیا اتفاق می‌افتد و در واقع تبدیل به یک سلاح برای کشورها شده است. پس برای آمادگی در مقابله با این شرایط، مهمترین نیاز، آموزش است.

نجفی‌ان: دلیل اینکه من در ابتدای صحبت‌م وارد مباحث فنی شدم دقیقاً همین بود. در تایید صحبت‌های مهندس محسنی‌نیا، باید اضافه‌کنم صرفاً خرید تجهیزات، عامل امنیتی بیشتر و مقابله با تهدیدات نیست. در بحث امنیت سه عامل مهم و اساسی وجود دارد. اول نیروی انسانی، دوم به‌کارگیری روال‌هایی چون ISMS و در نهایت تکنولوژی. اما متأسفانه اولین اقدام هر سازمانی تنها خریداری تکنولوژی و تجهیزات است!

در حالی نیروی انسانی به عنوان مهمترین عامل ناامنی شناخته می‌شود که کم هزینه‌ترین راه حل برای تامین امنیت شبکه هم همین نیروی انسانی است. مرحله بعدی از تامین امنیت، ایجاد روال‌های متعارف در سازمان است. مثلاً اگر قرار است سندی رد و بدل و امنیت آن هم حفظ شود، باید طبق روال خاصی انجام شود. ISMS در واقع معرفی استانداردها و ایجاد روال‌های امن در سازمان است. مرحله سوم و آخر، استفاده از تکنولوژی و تجهیزات امنیتی است. اما متأسفانه در ایران، سازمان‌ها در اولین قدم برای

عنوان یک مرجع مشخص به آن مراجعه کند. در واقع این مسئله که بخش خصوصی کسی را به عنوان صاحب و متولی بحث امنیت اطلاعات نمی شناسد، مشکل اصلی است. شاید باید این متولی حتی یک سطح بالاتر از دولت، نهادی مثل شوراهای عالی باشد.

صالحی: یعنی ما نیاز به یک نهاد فرا حاکمیتی - فرا بخشی داریم تا به طور کلان وارد عمل شود؟

قنبری: ما اولین کشور نیستیم که مورد حملات سایبری قرار می گیریم. بالاخره کشورهای دیگر هم تسهیلاتی برای مقابله با این حملات به کار گرفته اند. یعنی اگر بخش حاکمیتی بخواهد در این بخش سرمایه گذاری کند، دانش نهفته، مخفی و غیر قابل دسترسی نیست. صنایع موشکی ما چطور پیشرفت کرد؟ بالاخره عده ای دانش موجود در این کار را کسب، بومی کرده و ارگانی به عنوان متولی آن‌ها را یکجا جمع آوری و به سامان رسانده است. قطعاً در این راه سپاه پاسداران برای تامین کلیه ابعاد تاسیسات موشکی اش، به تنهایی وارد عمل نشده و با شرکت‌های خصوصی هم تعامل داشته است. در مورد فضای سایبر هم می توان این کار را کرد. در حالیکه حساسیت آن به مراتب از تاسیسات هسته ای و موشکی کمتر است.

محسنی نیا: دقیقاً باید کارها از حالت جزیره‌ای فعلی بیرون بیاید و با بهره گیری از تجربیات یکدیگر به نتیجه برسیم.

سعیدی: پیشنهاد همگی ما این است که دولت باید برای مقابله با تهدیدات سایبری از بخش خصوصی حمایت کند. اما نکته مهم اینکه در خارج از کشور، شرکت‌های خصوصی همکاری گسترده‌ای با بخش دولتی دارند. در حالیکه در ایران بخش خصوصی باید با چنگ و دندان سهمش از بازار را بگیرد. به نظر من در این زمینه شرکت‌های خصوصی باید با تعامل بیشتر با یکدیگر همکاری کرده و مطالباتشان را مطرح کنند. البته سازمان نظام صنفی هم باید از حرکت خودجوش شرکت‌ها برای ایجاد ضابطه استفاده کند. مثلاً یکی از اتفاقات مثبت در حمایت از تولید کننده داخلی، اختصاص بیلبردهای تبلیغاتی شهری به آن‌ها بود. این اقدام یک فرصت و حرکت مناسب برای حضور شرکت‌های داخلی و ایجاد یک ظرفیت برای آن‌ها است. راهکارهای ما هم باید از گذر نظام صنفی باشد و صنف به عنوان نماینده شرکت‌ها، خواسته‌های ما را مطرح کند.

محسنی نیا: من فکر می کنم می توان این کار را به عنوان یکی از وظایف کمیسیون افتای نظام صنفی قرار دهیم تا حداقل پیشنهادات ما در این زمینه به گوش شرکت فناوری اطلاعات برسد.

صالحی: جنس این پیشنهاد چیست؟ اینکه ما بخش دولتی را آگاه کنیم؟

محسنی نیا: نه! آگاه هستند، بلکه به یکدیگر اعتماد ندارد و هر یک می خواهند خودشان در راس کار باشند.

صالحی: خیلی از سازمان‌های دولتی این اتفاقات را ثبت می کنند اما متأسفانه در اغلب موارد این اطلاعات بدون تحلیل و بررسی رها می شوند.

سعیدی: دو هفته پیش با سازمانی تماس گرفتم و پیگیر سندی شدم که قرار بود برایشان ارسال کنیم. گفتند اینترنت ما قطع است لطفاً برای ما پست کنید. اگر اینترنت قطع است، پس اصلاً کار نمی کنید! یعنی میلیاردها تومان برای نیروی انسانی بیکار هزینه می کنیم. کارمندی در یک مجموعه دولتی به ما گفت، طی بخشنامه‌ای به آنها اعلام کرده اند، اگر سیستم کسی آلوده به ویروس فلیم باشد، اخراجش می کنیم، ما هم سیستم‌ها را خاموش کردیم و بیکارنشسته‌ایم!

متأسفانه مشکلی که ما در حال حاضر با آن روبرو هستیم، با محصول داخلی یا خارجی خریدن حل نمی شود. قبل از هر چیز باید به فکر آموزش نیروی انسانی باشیم. نیروی انسانی آموزش دیده، کارایی ابزارها را هم بیشتر می کند.

هنوز هم سازمان‌های صنعتی دنبال ویروس استاکس نت در سیستم‌هایشان هستند و هر ویروسی را استاکس نت خطاب می کنند. اما در نهایت مشخص می شود که عامل انسانی باعث نفوذ و افشای اطلاعات بوده است. تا زمانی که نیروی انسانی کارآمد نداشته باشیم، از بهترین تجهیزات امنیتی هم که استفاده کنیم، فایده‌ای ندارد و فقط آبروی شرکت داخلی و خارجی تولیدکننده می رود!

به جای درد دل، راهکار بدهیم

محسنی نیا: به نظر من ما در حال درد دل کردن هستیم. با توجه به اینکه کشور تا این حد مورد حمله جاسوسی قرار می گیرد، بهتر است به دنبال راهکار باشیم. متأسفانه ما عادت کرده‌ایم جزیره‌ای کار کنیم. اگر اطلاعات امنیتی همه سازمان‌ها، متمرکز و یکجا جمع آوری شود، تحلیل شده و در نهایت به اطلاع همه برسد، نتیجه بهتری خواهیم گرفت. کشورهای اروپایی هم مورد حمله جاسوسی قرار می گیرند و این اتفاق فقط مختص ایران نیست. سازمانی که متولی جمع آوری اطلاعات است باید پروتکل و جلساتی هم با کشورهای دیگر داشته باشد تا بتوان با نگاه بین‌المللی مشکلات را مطرح کرد.

قنبری: ضمن تایید صحبت‌های شما مثالی می زنم! در بحث ترافیک تهران، ارگان‌های مختلفی از جمله سازمان راهنمایی و رانندگی و شهرداری تهران درگیر هستند. هر کدام هم به صورت مستقل و جزیره‌ای کار می کنند. در واقع هیچ مرجعی برای پاسخگویی به مشکلات ترافیک تهران وجود ندارد. در بحث حملات و نفوذ هم نهاد و متولی مشخصی برای پاسخگویی نداریم. سازمان فناوری اطلاعات، ارتباطات زیرساخت، مرکز تحقیقات مخابرات، وزارت اطلاعات و... همه به صورت موازی و در کنار هم فعالیت می کنند. البته شورای عالی مجازی هم جدیداً در فضای گسترده‌تری شروع به فعالیت کرده است اما بیشتر بر مباحث فرهنگی تاکید دارد. ما نیاز به یک نهاد و تشکیلات منسجم داریم تا هم بخش خصوصی و هم بخش دولتی به



علیرضا صالحی

قوی دارند که می‌توانند تجهیزات را نصب و راهاندازی کرده و پول بگیرند. ولی دانشی به سازمان هدف منتقل نمی‌کنند. در حال حاضر تجهیزات بسیار گران قیمتی در ایران وجود دارد که امکان بروز رسانی آن قطع است. یعنی اصل کار مشکل دارد.

نجفیان: باید روال و روندی را ایجاد کرد تا طی آن، هم محصولات خارجی و هم تولیدات داخلی در شرایط واقعی و یکسان آزمایش شوند.

صالحی: به نظر شما این بخش ماجرا دقیقاً به دانش مصرف‌کننده مربوط نیست؟

محسنی‌نیا: متأسفانه همه بدون هیچ پشتوانه علمی خاصی فکر می‌کنند، فایروال خارجی خوب است ولی فایروال ایرانی بد است. در بسیاری از آزمون‌های دنیا، فایروال فورتی‌نت جزء پرفروش‌ترین UTM‌های دنیا شناخته شده است. در واقع مبدع فایروال در دنیا فورتی‌نت است. حالا این شرکت ادعا می‌کند ۸ گیگ ترابایت دارد. آیا این ادعا در شرایط واقعی هم حقیقت دارد؟ آزمایشگاه NSS LAB که در دنیا جزء بهترین و مجهزترین آزمایشگاه‌ها است، طبق شرایط واقعی تجهیزات امنیتی را بررسی می‌کند. طبق متدولوژی این آزمایشگاه، ۸ گیگ ادعای فورتی‌نت به ۱۵۰ مگابایت رسیده است. در حالیکه این شرکت همچنان به خودش افتخار می‌کند که از آزمون NSS LAB با موفقیت بیرون آمده است.

واقعیت این است که خیلی از سازمان‌های ما دانش لازم در این زمینه را ندارند و ما به عنوان تولیدکننده داخلی فرصت می‌خواهیم خودمان را در بازار نشان دهیم. اما متأسفانه مصرف‌کننده این فرصت را به ما نمی‌دهد. مثالی می‌زنم. اگر تجهیزات ما در شبکه یک سازمان دولتی قرار گرفته باشد، مشکل موجود در شبکه را گردن تجهیزات ما می‌اندازند اما اگر یک وسیله خارجی در شبکه باشد و شبکه همان مشکل را داشته باشد، می‌گویند شبکه یعنی همین!

خدا را شکر محصولات داخلی با سرمایه خودشان رشد کردند. اما نیاز به حمایت دارند. هدف ما این نیست بگوییم محصولات خارجی خوب نیست اما اطمینان داریم محصولات داخلی، هم‌تراز با نمونه‌های خارجی هستند.

کنکوری واقعی برای همه

صالحی: شما بیش از حد توان از مشتری انتظار ندارید؟ مشتری وظیفه آزمایش محصول را ندارد. اما شما از مشتری می‌خواهید که بفهمد محصول ایرانی بهتر است و همان را هم بخرد. چرا مشتری باید در این زمینه سرمایه‌گذاری کند؟

نجفیان: اگر چه تعداد مراکزی که محصولات را آزمایش می‌کنند کم است اما وجود دارند. باید روال و روندی را ایجاد کرد تا طی آن، هم محصولات خارجی و هم تولیدات داخلی در شرایط واقعی و یکسان آزمایش شوند.

محسنی‌نیا: لطفاً جایی را هم در کشور به ما معرفی کنید که محصولات خارجی را آزمایش می‌کنند و رتبه می‌دهند. متأسفانه غرب‌زدگی از همین جا شروع می‌شود. چطور محصول خارجی ادعا می‌کند که بهترین است و همه هم این



عالم نجفیان

سعیدی: یکی از پیشنهادات مثبت سازمان نظام صنفی، گروه‌بندی شورای عالی انفورماتیک بود. دولت هم این پیشنهاد را قبول کرد و با توجه به وظایف هر شرکت گروه‌بندی انجام شد. به نظر من باید طی یک برنامه زمان‌بندی مشخص، نظام رتبه‌بندی شرکت‌ها را پیاده‌کنیم تا با تشخیص دولت، قابلیت‌های هر شرکتی مشخص شده و با توجه به آن، از توانمندی شرکت‌ها استفاده کنند. با ایجاد پروتکل ارتباطی در این زمینه، شرکت‌ها دیگر به فکر از

میدان به در کردن یکدیگر نیستند و در کنار هم در بازار رقابت خواهند کرد. این مسئله باعث می‌شود شرکت‌ها هم با برنامه وارد بازار شده و از هرج و مرج هم جلوگیری شود. ما باید در حالیکه ظرفیت‌های خود را به بازار معرفی می‌کنیم از دولت هم بخواهیم بازار را برای ما آماده کند. اما متأسفانه خودمان هم در صنف، منفعلانه عمل می‌کنیم.

به عنوان مثال نظام صنفی در حالی بحث ساماندهی بازار محصولات خارجی را مطرح می‌کند که هنوز نتوانستیم بازار داخل را ساماندهی کنیم. این نشان دهنده این است که ما هیچ برنامه مدون و مشخصی نداریم. جلساتی هم که در نظام صنفی برگزار می‌شود تنها به تازه شدن دیدارها می‌گذرد و هیچ خروجی مشخصی ندارد.

محسنی‌نیا: متأسفانه نظام صنفی ما بسیار ضعیف عمل می‌کند. من نظام صنفی را با تشکل نظام مهندسی ساختمان مقایسه می‌کنم. این تشکل قدرت وضع قانون دارد. مثلاً قانونی وضع کرده‌اند که اگر هر زمانی دلار بالا رفت حتی اگر قرارداد با قیمت قبلی منعقد شده باشد، همه قیمت‌های مندرج در قرارداد براساس نرخ روز دلار محاسبه خواهد شد. در واقع آن نظام صنفی آنها آنقدر به دولت فشار آورده که این مسئله را تبدیل به قانون کرده است. اما وقتی ما با شرکت‌های دولتی قرارداد می‌بندیم، در خوش‌بینانه‌ترین حالت، ۱۰ درصد بعد از عقد قرارداد پرداخت می‌کنند. در حالیکه من به عنوان تولیدکننده باید ۹۰ درصد سرمایه‌گذاری کنم.

صالحی: به نظرم بحث دوباره حالت درد دل پیدا کرد. من می‌خواهم بحث را به جایی ببرم که مشخص شود بخش خصوصی باید چه مطالباتی از بخش دولتی داشته باشد؟

محسنی‌نیا: من توضیحی در مورد بازار محصولات داخلی بدهم. یک ابزار خارجی قوی با پشتیبانی قوی را با یک ابزار بومی که ۷۰ درصد قابلیت و

توانایی یک ابزار خارجی را دارد، مقایسه کنید. نکته مهم در این دو محصول میزان توانایی آن‌ها نیست بلکه مهم قرار گرفتن تولیدکننده پشت ابزار داخلی است. یعنی اگر مشکلی به وجود بیاید، مشتری حتی می‌تواند مستقیم با مدیر عامل تماس بگیرد تا مشکل حل شود. به نظر من واردکنندگان تجهیزات خارجی بیشتر به کار دلالتی مشغولند. شما برای من یک شرکت بزرگ مثال بزنید که ضمن داشتن دانش قوی، فروشنده تجهیزات خارجی هم است. اصلاً نداریم. چرا که آنها فقط یک تیم پشتیبانی

تک سازمان‌های دولتی نسبت به خرید محصول و تجهیزات امنیتی تعیین تکلیف کند. از اینجا به بعد به فرهنگ و دانش خود خریدار بستگی دارد. اینکه کمک کنند حتی اگر نقطه ضعفی دارید، این ضعفها برطرف شده و همچنان سرپا باقی بمانید

محسنی‌نیا: اگرچه فرهنگ‌سازی و حمایت‌های دولتی بسیار مهم است اما ضرب‌المثلی داریم که می‌گوید کس نخارد پشت من جز ناخن انگشت من! خدما باید شروع

کنیم. اول باید فرهنگ خودمان را اصلاح کنیم. مثلاً سمیناری بگذاریم و دانش‌مان را منتقل کنیم. هزینه‌ای هم برای این کار از سازمانی دریافت نکنیم تا فکر نکنند برایشان کیسه دوخته‌ایم. با این کار وقتی شما حرفی بزنید قبول می‌کنند و یا حداقل برای خرید محصول از شما مشاوره می‌گیرند. باید کاری کنیم که اعتمادها به سمت ما جلب شود. چراکه پیش زمینه فرهنگی ما عدم اعتماد به یکدیگر است.

نجفیان: مهم است که شرکت‌های تولیدی بدون تبلیغ برند خاصی به صورت مشترک، تنها به تبلیغ محصولات داخلی بپردازند.

صالحی: به نظر من هم برگزاری سمیناری در حد انتقال دانش به مشتریان بسیار مهم و اساسی است.

محسنی‌نیا: من یک نکته دیگر هم اضافه کنم. هر شرکتی که در ایران فایروال تولید می‌کند، برای تولیدش نیاز به کسب مجوز از طرف سازمان فناوری اطلاعات دارد. پیشنهاد من این است که محصولات خارجی هم برای عرضه در بازار نیاز به کسب چنین مجوزی از شرکت فناوری اطلاعات داشته باشند.

قانونی داریم که اگر یک محصول خارجی، نمونه داخلی داشته باشد، مثل لوازم خانگی و صوتی تصویری، وارد کننده محصول خارجی، باید ۶۰ درصد حق گمرک بپردازد. اما برای واردات تجهیزات امنیتی شبکه که نمونه داخلی هم دارد، چنین قانونی نداریم.

فرهنگ را با حرف نمی‌توان عوض کرد؛ باید وارد عمل شویم. من در محیط عملیاتی نشان خواهم داد که محصول ایرانی بهتر است. اما آیا می‌توانم برای هر مشتری چنین تشکیلاتی راه بیندازم؟ پس باید سازمان مشخصی به عنوان متولی اصلی اینکار معرفی شود.

سعیدی: به نظر من بد نیست که تولیدکنندگان ایرانی هم هرازگاهی هزینه‌ای کرده و در آزمون‌های بین‌المللی شرکت کنند

قنبری: به نظر من هم برگزاری سمیناری مشترک بین تولیدکنندگان داخلی برای انتقال دانش فنی می‌تواند در جلب اعتماد مشتریان و خرید تولیدات داخلی روش موثری باشد.

سعیدی: به نفع مردم است که محصول داخلی بخرند. منطقی‌ترین علت آن هم این است که وقتی محصول مشکلی پیدا کند، دستشان به تولید کننده می‌رسد.

مسئله را قبول می‌کنند اما من هموطنی که این ادعا را دارم کسی به من اعتماد نمی‌کند؟ باید در یک شرایط یکسان، هم محصولات خارجی و هم محصولات داخلی آزمایش شوند و یک کنکور واقعی از همه بگیرند. نه اینکه تولیدکننده خارجی کارنامه قبولی‌اش را در دست داشته باشد و به همه نشان دهد اما از ما امتحان‌های خیلی سختی گرفته شود. از محصول داخلی انتظار دارند کل حملات را شناسایی کند. آیا محصول خارجی هم تضمینی برای شناسایی کل حملات دارد؟

سعیدی: به نظر من شرایط فعلی ما حکم ماشین زهوار در رفته‌ای را دارد که ظرف مدت زمان کوتاهی هم اصلاح نمی‌شود. باید همه بخش‌ها به بلوغ برسند تا مشکلات برطرف شود. این مسئله مشکل تک تک ما است. یاد گرفته‌ایم تا وقتی می‌شود چیزی را مجانی به دست آورد، چرا پول بدهیم؟ اما اصلاً به ضعف شدن صنعت فکر نمی‌کنیم. به نفع مردم است که محصول داخلی بخرند. منطقی‌ترین علت آن هم این است که وقتی محصول مشکلی پیدا کند، دستشان به تولید کننده می‌رسد.

صالحی: این دقیقاً به همان مسئله فرهنگ سازی برمی‌گردد. خریدار هنگام خرید، فارغ از داخلی یا خارجی بودن محصول باید دقت کرده و سپس تصمیم‌گیری کند. اما نباید بعد از خرید محصول داخلی بیش از حد سختگیری کند و چون تولیدکننده نزدیکش است، برای هر مسئله کوچکی نسبت به خرید محصول ابراز پشیمانی کند.

سعیدی: اگر دولت ما هم مثل سایر کشورها به مالکیت معنوی و حمایت از تولیدکننده پایبند باشد، مشکلات برطرف می‌شوند. یک نویسنده در اروپا با نوشتن یک کتاب، زندگی‌اش به کلی دگرگون می‌شود اما اینجا تولیدکنندگان داخلی به راحتی ورشکسته می‌شوند.

محسنی‌ان: به نظر من بهتر است علاوه بر بحث فرهنگ سازی و همچنین حمایت‌های دولتی، به این مسئله هم بپردازیم که شرکت‌های خصوصی خودشان باید برای خودشان چه کاری انجام دهند. به نظر من شرکت‌های خصوصی قبل از هر چیز باید دانش خود را به سازمان‌ها منتقل کنند. باید تفکر سازمان‌ها را عوض کنند. چرا که سازمان‌های دولتی ندانسته و از روی عدم دانش نسبت به خرید محصول خارجی تصمیم‌گیری می‌کنند.

متأسفانه خودمان در جانداختن این فرهنگ غلط که محصول خارجی بهتر از ایرانی است، اشتباه عمل کرده‌ایم. باید قبل از هر چیز این نگاه را اصلاح کنیم. توضیح‌دهیم که ممکن است محصول شما بروز نشود و حتی هنگام بروز رسانی، از آنجائیکه می‌دانند در ایران هستید، هزاران ویروس و بدافزار دیگر هم همراهش بفرستند. حتی ممکن است محصول خارجی قوی باشد، اما نیاز شما را برطرف نکند

سعیدی: نباید از حق بگذریم، دولت نمی‌تواند برای تک



حمیدرضا سعیدی