برای حضور در بازار داخلی فرصت می‌خواهیم

میزگرد بررسی توانمندی‌های داخلی در مقابله با تهدیدات سایبری


محمود محسنی نیا


کاظم قنبری


عامر نجفیان


حمیدرضا سعدی


علیرضا صالحی

- آنتی ویروس‌های خارجی پالایش می‌شوند
- هر روز ۷۰ هزار حمله سایبری
- فرهنگ‌سازی در فضای سایبر
- جاسوس چند چهره

رئیـس کمیسیـون افتـــای سازمـــان نظام‌صنفـی رایـانـه‌ای خبـــر داد

آنتی‌ویـــروس‌های خـارجی پالایـش می‌شـوند

رئیس کمیسیون افتـا سازمان نظام صنفـی رایانـه‌ای تهـران گفت: با اعلام ممنوعیت ورود ضدبدافزارهـای خارجی، قرار شد به موازات حمایت از تولید ضدبدافزارهای بومی از برخی آنتی‌ویروس‌های خارجی برای تأمین امنیت استفاده شود.

بهناز آریـا 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 افتـای سازمان نظام صنفـی رایانـه‌ای 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 هیئت مدیره سازمان نظام صنفی رایانه‌ای استان تهران گفت: در این زمینه طی جلساتی با معاون گسترش سازمـان فناوری اطلاعات، قرار شد برای راه‌حل میان‌مدت، در مرحله نخست از برخی آنتـی‌ویروس‌های خارجی برای تأمین امنیت استفاده شود و به موازات آن تولید و استفاده از ضدبدافزارهای تولید داخل نیز حمایت و پیگیری گردد.

آریـا گفت: از این رو با همکاری مشترک سازمان فناوری اطلاعات ایران و کمیسیون افتای سازمان نظام صنفی رایانه‌ای استان تهـران، "کارگروه ساماندهی ضد بدافزارهای خارجی" تشکیل شد که جلسـات 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 لحـاظ کردن ملاحظات حاکمیتی و ملی، ضد بدافزارهای اعلام‌شده را مورد ارزیابی قرار می‌دهد و در نهایت ضدبدافزارهای مورد تایید اعلام می‌شوند.

عضو هیئت‌مدیره سازمان نظام صنفی رایانه‌ای استـان تهران تأکیـد کرد: در این مرحله بازار هدف صرفـا سازمان‌های دولتی قـرار داده شـده که باید ضد بدافزارهـای خود را از لیست اعلامی و مورد تایید سـازمـان فنـاوری اطلاعات انتخـاب نمایند.

وی ادامه داد: علاوه بر این، شناسـایی و تعیین ملاک‌های ارزیابی شرکت‌های عرضه کننده این محصـولات 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 ادامـه داد: دراین فراخـوان شرکت‌هـای واردکننـده و فروشنـده ضدبدافزارهای خارجی که با سازمان‌های دولتی همکاری دارند، باید اطلاعات خود را به صورت خوداظهاری به ثبت برسانند.

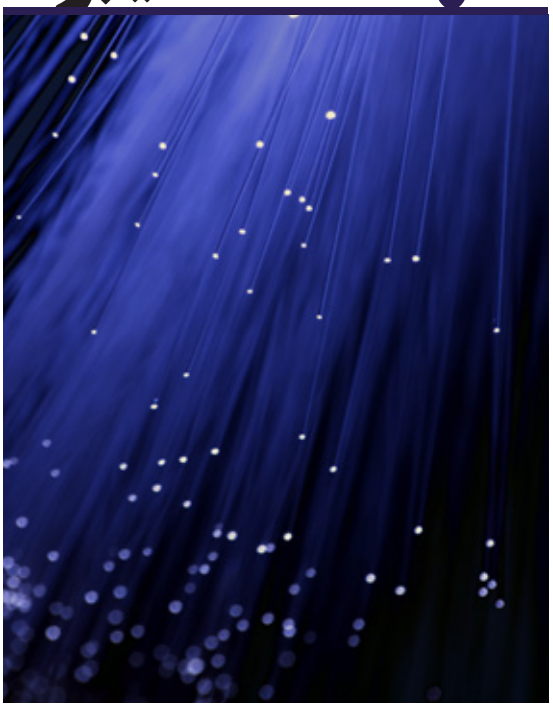
وی ادامه داد: با تشکیل بانک اطلاعاتی شرکت‌ها و برندهای واردکننده ضدبدافزارهای خارجی، ارگان‌های دولتی با مراجعه به آن قادر خواهند بود مطابق با نیاز سازمانی‌شان نرم‌افزار و خدمات امنیتی را از شرکت‌هایی که اسامی آنها در این بانک اطلاعاتی ذکر شده و صلاحیت‌شان به تایید رسیده سفارش دهند.

آریـا گفت: در مرحلـه بعد نیز اطلاعات خوداظهـاری شرکت‌ها با واقعیت تطبیق داده خواهد شد.

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

مـعـــاون وزیـــر ICT خبـــر داد:

۷۰ هـزار حمله سایبری هر روز



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

علی حکیـم‌جوادی درباره‌ی حملات سایبری اظهـار کرد: اکنون هیچ کشوری در دنیا وجود ندارد که بگوید تاکنون با حملات سایبری مواجه نشـده است، چراکه در حـال حاضر از یک هکـر آمـاتور تا هکرهای سازمان یافته و گاه دولت‌ها هم می‌توانند مزاحمت‌هایی برای سایر کاربران ایجاد کرده و حتی به زیرساخت‌های حیاتی کشورها حمله کنند.

رییس 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 داشتـه باشـد.

حکیم‌جوادی در ادامه راه‌اندازی مرکز "ماهـر" را اقدامی در همـین راستـا دانست و خاطـر نشان کرد: نباید تعـداد حملات به چنـد حمله محـدود خلاصه شود، امـا با این حال تفـاوت‌های عمده‌ای بین حمله‌هـای صورت گرفتـه وجـود دارد و این حمله‌هـا گـاه به گونـه‌ای بـوده است که نمی‌تـوان آن را از طریق یک فـرد ارزیابی کـرد، چراکه سرمـایه‌گذاری‌هـای بسیاری برای آن‌ها صورت گرفته است.

رییس سازمان فن‌آوری اطلاعات در ادامه با تاکید بر این‌که تاکنون با تحقیقات و تلاش‌های صورت گرفته کارشناسان موفق به شناسایی سـریع ویروس‌هـا و بدافزارهای مهـاجم شده‌انـد، گفت: یکی از راهکارهایی که می‌توان برای جلوگیری از گسترش این موضوع مورد استفـاده قـرار 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 کشـورها این مسالـه را یکی از تهدیدهای خود عنـوان کردند و حتی برخی کشورها آنقدر برروی این موضوع حسـاسیت نشان دادند که این حملات را در حد نظامی ارزیـابی کردند.

او ادامه داد: خوشبختـانه اکنون همکاری‌هـای خوبی بیـن فعالان حـوزه‌ی سـایبر صورت گرفته و ما امیدواریم با همکاری‌های بیش‌تـر دست‌اندرکاران پاسخ به‌موقعی برای این تهدیدهـا داشته باشیم.

حکیـم‌جوادی در عین حـال راه‌انـدازی شبکـه ملی اطلاعـات و دسـترسی بخش‌های اجرایی به شبکـه‌ای برون‌مـرزی را یکی از راهکـارهای مهم کاهش این خطر برشمـرد.

عـامل پیشگیـری از وقـوع جـــرم:

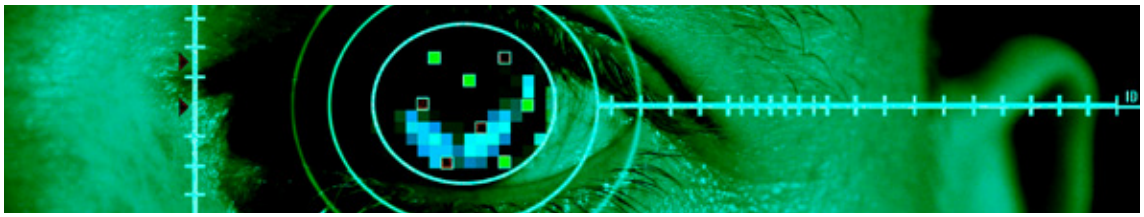
فـرهنگ سـازی در فضای سایبـر

رئیس پلیس فتا با اشاره به اینکه فرهنگ سازی استفاده از فضای سایبری عامل پیشگیری از وقوع جرایم می‌باشد، 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 رقابت‌های 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.

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 می‌سازد، 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 نمونه‌های پیشگیری از شکل گیری جرایم در فضای مجازی است.



معـاون وزیـر ICT خبـــر داد:

دستور رییس جمهوری برای استخدام نیـــرو در حـــوزه امنیت اطلاعـــات

معاون وزیر ارتباطات و فناوری اطلاعات از دستور رییس‌جمهوری برای جذب نیروهای انسانی در زمینه‌ی امنیت فن‌آوری اطلاعات خبر داد.

علی حکیم جوادی، رییس سازمان فن‌آوری اطلاعات، گفت: مدتی است برای تامین امنیت بیشتر، رییس‌جمهور دستور جذب نیروهای انسانی مورد نیاز در زمینه‌ی امنیت فن‌آوری اطلاعات را صادر کرده و قرار است این نیروها از طریق معاونت توسعه نیروهای ریاست‌جمهوری 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 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.

حکیم‌جوادی در بخش دیگری از صحبت‌های خود هم به ارائه الکترونیکی خدمات دولتی اشاره کرد و گفت: قرار بود تا پایان سال ۹۱تمام بخش‌های اجرایی به شبکه‌ی ملی اطلاعات متصل شوند که با دستور رییس‌جمهوری قرار بر آن شد که در این موضوع تسریع شود و تا دو ماه دیگر تمام دستگاه‌ها به این شبکه متصل شوند.

تحلیـل آزمایشگـاه ضـد بدافـزار ایمـن از بـدافزار فلیـم

جاسوس چند چهره

بعـد از حملـه سـایبری به شرکت نفت آزمـایشگاه ضدبـدافزار ایمن که نخستیـن آزمایشگاه ضدبدافزار ایرانـی می‌باشـد خـود را موظف دانست تا همـانند حملاتی همچـون استـاکس‌نت باز به دنبـال راه‌های شنـاخت و مقابلـه با این بـدافزار باشـد.

می‌توان ویروس شعله را در میان بدافزارها و جاسوس‌افزارها یکی از خطرناک‌ترین ومخربترین 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 ظاهرا هر اقدامی را برای مهاجمان فراهم می‌سازد.

جمع آوری اطلاعات و فرستادن آنها، نفوذ در شبکه‌های بزرگ (گاها صنعتی و مهم) ، از بین بردن اطلاعات سیستم آلوده، قدرت جست‌وجو، تحلیل و پردازش گونه‌ای 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 می کند 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 تائید 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.

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 انجام‌شد، کمتر کسی فکر می‌کرد، بدافزارها و ویروس‌های‌جاسوس روزی بتوانند بدون هیچ جنگ و خونریزی به عنوان یکی از بزرگترین و قدرتمندترین روش‌های حمله به کشورها تلقی‌شوند.

طی سال‌های اخیر و به‌ویژه با گسترش فعالیت‌های هسته‌ای ایران، یکی از کانون‌های اصلی و همچنین مرکز توجه نفوذگران، ایران و فعالیت‌های هسته‌ای آن بوده‌است. 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 طراحی‌شد. 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 گو را بخوانید.

صالحـی: دو سال قبل ویروسی به نام استاکس‌نت به عنوان یکی از جدی‌ترین تهدیدات سایبری وارد کشور شد. حالا بعد از گذشت زمان، شاهد تهدیدات جدیدتری چون ویروس فلیم هستیم. در میزگرد امروز می‌خواهیم به بررسی توان تولیدکنندگان داخلی در مقابله با تهدیدات سایبری بپردازیم. متاسفانه یکی از مهمترین دغدغه‌های مدیران شرکت‌های بخش خصوصی صرف نظر از راهکارهای داخلی یا خارجی برای مقابله با تهدیدات، عدم همکـاری بخش دولتـی در این زمینه است. برای شروع لطفاً هر یک از مدیران که در این زمینه تجربه‌ای دارند بفرمایند.

سعـدی: متاسفانه 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 تاثیر مخرب شان بر شبکه ما وارد شد، شناسایی و تحلیل می‌شوند. مثلاً در مورد ویروس استاکس نت، کارشناسان پس از گذشت یک‌سال که آسیب‌های زیادی به شبکه‌ها 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 می‌شوند، سرورهای داخلی ما روزانه بین ۴۰ تا ۵۰ هزار بدافزار را جمع‌آوری می‌کنند که بین آن‌ها ممکن است چندین جاسوس‌افزار 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 امکان‌پذیر نیست. با اینکه ویروس فلیم بهمن ماه شناسایی شد اما تحلیل و بررسی عملکرد آن از دو هفته قبل (اواسط تیرماه) انجام شد.

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

صالحـی: برخورد سازمان‌ها در زمان کشف ویروس چگونه است؟ آیا برخورد حراستی است؟ آیا به کارشناسان شما برای بررسی و نمونه‌برداری اجازه ورود به سـازمان داده می‌شود؟

سعـدی: دقیقاً مشکل ما در آزمایشگاه همین است. به دلیل رسالت آزمایشگاه مهران‌رایانه، هر سازمانی بعد از بروز مشکل با ما تماس می‌گیرد. اما متاسفانه نه برای تحلیل ویروس هزینه‌ای پرداخت می کنند و نه تمایلی به رسانه‌ای شدن موضوع دارند.

قنبـری: در سایر کشورها با یک روال مشخصی مثلاً داشتن امضا و یا نشانه، کارشناسان مرتبط حق ورود به سازمان و نمونه‌برداری دارند. اما در کشور ما اگر در سازمان اطلاعاتی هم در مورد ویروس وجود داشته باشد، به دلایل امنیتی مشکل را سربسته مطرح کرده و می‌ترسند اطلاعاتی در اختیار ما قرار دهند!

قنبـری: بزرگتـریـن ویروسـی کـه تاکنـون باعث خروج اطلاعات از سازمان شده و به عنوان یک تهدید مهم شناخته می‌شـود، ویروس دوپـا یا همـان نیروی انسانی شاغل در سازمان‌ها است.

محسنی‌نیـا: بحث ویروس‌ها و بدافزارهای جاسوسی نظیر استاکس نت و فلیم تمام شدنی نیست و نه تنها برای ایران بلکه در کل دنیا اتفاق می‌افتد. به نظر من باید در این جلسه به دنبال راهکارهایی باشیم تا اجازه ندهیم، بیشتر از این به ما صدمه بزنند.

قنبـری: به نظر من بزرگترین ویروسی که تاکنون باعث خروج اطلاعات از سازمان شده و به عنوان یک تهدید مهم شناخته می‌شود، ویروس دوپا یا همان نیروی انسانی شاغل در سازمان‌ها است. اما متاسفانه ما همیشه به دنبال فرار از این واقعیت بودیم و سعی می‌کنیم همه خطاها را به گردن ویروس بیاندازیم.

یک تیم تخصصی پشت ویروس فلیم

نجفیـان: 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 ضدویروس و فایروال وایجاد شبکه‌های 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. تقریبا همه تائید می‌کنند ویروس فلیم، یکی از قوی‌ترین ویروس‌هایی بوده که تاکنون نوشته شده است. به نظر من تیمی که این ویروس را نوشته، یک تیم ویروس‌نویس صرف نبوده بلکه هر بخش آن توسط تیمی متخصص نوشته شده است.

ویروس فلیم برای ورود به سیستم، الگوریتم MD5 ویندوز را هک می‌کنـد. چند سال قبل متخصصان قابل نفوذ بودن MD5 را به مایکروسافت تذکر دادند. مایکروسافت هم این امکان را از همه بخش‌های ویندوز به جز بخش Auto Update حـذف کـرد. ویروس فلیم هم دقیقـاً از همین نقطه، سوءاستفاده کرد. این ویروس روی بخش Auto update ویندوز نشسته و اصلاحیه‌های مایکروسافت را می‌گیرد. خودش هم چند فایل دیگر به آن اضافه می‌کند.

از آنجائیکه فایل‌های اضافی در کنار اصلاحیه‌های مایکروسافت امضا می‌شوند، هیچ ضدویروسی نمی‌تواند فایل‌های مخرب را از سایر فایل‌ها تشخیص دهد. کاربران همه فایل ها را نصب می‌کنند، بی خبر از اینکه فایل‌های مخرب هم بین آن‌ها وجود دارد. با این توضیح می‌خواهم به این نتیجه برسم که این تکنیک‌ها فراتر از یک ویروس نویسی ساده است.


کاظم قنبـری

قنبـری: قطعا دانش ویروس‌ها و ویروس نویس‌ها به مرور زمان بیشتر شده است اما مشکلی که به‌ویژه در سازمان‌های دولتی با آن روبرو هستیم این است که برای نفوذ به شبکه این سازمان‌ها نیازی به این همه پیچیدگی

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 گذاشته اند. به نظر من در شرایط فعلی شاید تکنولوژی پشت این ویروس ها آنقدر مهم نباشد. بلکه روندی که باید در سازمان‌ها تعریف شود تا اساسا نفوذ را غیرممکن کند، مهم‌تر است. به نظر من قبل از هرچیز 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 سازمان ها 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 دیدگاه‌هایی 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 ایمنی 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 متاسفانه 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. مثلا 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 متاسفانه در ایران، سازمان‌ها در اولین قدم برای تامین امنیت به فکر خرید تکنولوژی می افتند و با خریدن یک فایروال می‌خواهند امنیت همه جانبه‌ای برقرار کنند!

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

سازمان‌ها بعد از برقراری کلیه این جوانب، باید به دنبال پیاده‌سازی یک راه‌حل امنیتی هم باشند. مدتی است مبحثی 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 می‌توان پی به وقوع یک اتفاق مشکوک برد. ویروس‌های رایانه‌ای هم مثل ویروس سرماخوردگی به مرور بیشتر شده و کهنه می‌شوند. هرقدر سازمان دیرتر متوجه حضور و فعالیت آن‌ها شود، جلوگیری از گسترش اثرات مخرب آنها هم سخت‌تر خواهدشد. 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 چه‌کار 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 متاسفانه در اغلب موارد این اطلاعات بدون تحلیل و بررسی رها می‌شوند.

سعدی: 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 بهره‌ببرند. 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 واردعمل شود و نمره منفی را به سازمانی بدهد که برای جلوگیری از نفوذ، شبکه دو تکه طراحی‌کرده و کلا شبکه داخلی‌اش قطع‌است!


محمود محسنی‌نیا

صالحی: متاسفانه خیلی از سازمان‌ها اعتقاد دارند که تنها راه‌حل جلوگیری از نفوذ، داشتن یک شبکه دو تکه است.

سعـــدی: 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 نمی‌کنید! 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 می‌کنیم، ما هم سیستم ها را خاموش کردیم و بیکار نشسته‌ایم!

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

هنوز هم سازمان های صنعتی دنبال ویروس استاکس نت در سیستم‌هایشان هستند و هر ویروسی را استاکس نت خطاب می‌کنند. اما در نهایت مشخص می‌شود که عامل انسانی باعث نفوذ و افشای اطلاعات بوده است.

تا زمانیکه 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 جـــای درد دل، راهکـــار بدهیـــم

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

قنبـــری: ضمن تایید صحبت‌های شما مثالی می‌زنم! 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 می‌کنند. 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 می‌کنند. 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 عنوان یک مرجع مشخص به آن مراجعه کند.

صالحـــی: خیلـــی از سازمان‌هـــای دولتـــی ایـــن اتفاقـــات را ثبت می‌کنند اما متـــاسفانه در اغلب مـــوارد ایـــن اطلاعات بدون تحلیل و بررسی رها می‌شوند.

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.

صالحـــی: یعنی ما نیاز به یک نهاد فراحاکمیتی- فرا بخشی داریم تا به‌طور کلان وارد عمل شود؟

قنبـــری: ما اولین کشور نیستیم که مورد حملات سایبری قرار می‌گیریم. بالاخره کشورهای دیگر هم تسهیلاتی برای مقابله با این حملات به‌کار گرفته‌اند. یعنی اگر بخش حاکمیتی بخواهد در این بخش سرمایه‌گذاری کند، دانش نهفته، مخفی و غیرقابل دسترسی نیست. صنایع موشکی ما چطور پیشرفت کرد؟ بالاخره عده ای دانش موجود در این‌کار را کسب، بومی کرده و ارگانی به عنوان متولی آن‌ها را یکجا جمع‌آوری و به سامان رسانده است. قطعا در این راه سپاه پاسداران برای تامین کلیه ابعاد تاسیسات موشکی‌اش، به تنهایی وارد عمل نشده و با شرکت‌های خصوصی هم تعامل داشته است. در مورد فضای سایبر هم می توان این‌کار را کرد. درحالیکه حساسیت آن به مراتب از تاسیسات هسته ای و موشکی کمتر است.

محسنی‌نیـــا: دقیقاً باید کارها از حالت جزیره‌ای فعلی بیرون بیاید و با بهره‌گیری از تجربیات یکدیگر به نتیجه برسیم.

سعـــدی: 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 نظام‌صنفی هم باید از حرکت خودجوش شرکت‌ها برای ایجاد ضابطه استفاده کند.

مثلاً یکی از اتفاقات مثبت در حمایت از تولید کننده داخلی، اختصاص بیلبوردهای 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.


علیرضا صالحـــی

محسنی‌نیـــا: من فکر می‌کنم می‌توان این‌کار 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.

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

محسنی‌نیـــا: نه! آگاه هستند، بلکه به یکدیگر اعتماد ندارد و هر یک می‌خواهند خودشان در راس کار باشند.

سعـــدی: 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 استفاده‌کنند. 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 متاسفانه 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 می شود تنها به تازه شدن دیدارها می‌گذرد و هیچ خروجی مشخصی ندارد.

محسنی‌نیـــا: متاسفانه 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 خوش‌بیناترین حالت، ۱۰ درصد بعد از عقد قرار داد پرداخت می‌کنند. در حالیکه من به عنوان تولید کننده باید ۹۰ درصد سرمایه‌گذاری کنم.

صالحـــی: به نظرم بحث دوباره حالت درد دل پیدا کرد. من می‌خواهم بحث را به جایی ببرم که مشخص‌شود بخش خصوصی باید چه مطالباتی از بخش دولتی داشته‌باشد؟

محسنی‌نیـــا: 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 دلالی مشغولند. شما برای من یک شرکت بزرگ مثال بزنید که ضمن داشتن دانش قوی، فروشنده تجهیزات خارجی هم است. اصلا نداریم. چرا که آنها فقط یک تیم پشتیبانی 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.

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

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

محسنی‌نیـــا: متاسفانه همه بدون هیچ پشتوانه علمی خاصی فکر می‌کنند، فایروال خارجی خوب است ولی فایروال ایرانی بد است. در بسیاری از آزمون‌های دنیـا، فایروال فورتی‌نت جزء پرفروش‌ترین UTMهای دنیا شناخته شده است. در واقع مبدع فایروال در دنیا فورتی‌نت است. حالا این شرکت ادعا می کند ۸ گیگ تروپوت 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 تولید کننده داخلی فرصت می‌خواهیم خودمان را در بازار نشان دهیم. اما متاسفانه مصرف کننده این فرصت را به ما نمی دهد. مثالی می‌زنم. اگر تجهیزات ما در شبکه یک سازمان دولتی قرار گرفته باشد، مشکل موجود در شبکه را گردن تجهیزات ما می اندازند 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، همطراز با نمونه‌های خارجی هستند.

کنکـــوری واقعـــی بـــرای همـــه

صالحـــی: 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؟


عـــامر نجفیـــان

نجفیـــان: اگرچه 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.

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

مسئله را قبول می‌کنند اما من هموطن 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؟

سعـدی: به نظر من شرایط فعلی ما حکم ماشین زهوار در رفته ای را دارد که ظرف مدت زمان کوتاهی هم اصلاح نمی‌شود. باید همه بخش ها به بلوغ برسند تا مشکلات برطرف شود. این مسئله مشکل تک تک ما است. یاد گرفته ایم تا وقتی می شود چیزی را مجانی به دست آورد، چرا پول بدهیم؟ اما اصلاً به ضعیف شدن صنعت فکر نمی کنیم.

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.

صالحـی: این دقیقاً به همان مسئله فرهنگ سازی برمی‌گردد. خریـدار هنگام خرید، فـارغ از داخلی یا خارجی بـودن محصـول 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.

سعـدی: 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 می شوند.

محسنیـان: 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 تصمیم گیری می‌کنند. متاسفانه خودمان در جاانداختن 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 می دانند در ایران هستید، هزاران ویروس و بدافزار دیگر هم همراهش بفرستند. حتی ممکن است محصول خارجی قوی باشد، اما نیاز شما را برطرف نکند

سعـدی: نباید از حق بگذریم، دولت نمی‌تواند برای تک تک سازمان‌های دولتی نسبت به خرید محصول و تجهیزات امنیتی تعیین‌تکلیف 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

سعـدی: به‌نفـع مـردم است کـه محصـول داخلـی بخـرنـد. منطقی‌تـرین علت آن هم این است که وقتـی محصول مشکلـی پیدا کند، دستشان به تولید کننده‌می‌رسـد.

محسنی‌نیـا: اگرچه فرهنگ‌سازی و حمایت‌های دولتی بسیار مهم است اما ضرب‌المثلی داریم که می‌گوید کس نخارد پشت من جز ناخن انگشت من! خودمان باید شروع کنیم. اول باید فرهنگ خودمان را اصلاح کنیم. مثلاً سمیناری بگذاریم و دانش‌مان را منتقل کنیم. هزینه‌ای هم برای این‌کار از سازمانی دریافت نکنیم تا فکر نکنند برایشان کیسه دوخته‌ایم. با این‌کار 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.

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

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

محسنی‌نیـا: 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 امنیت 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.


حمیدرضا سعدی

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

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