افتای ایرانی
درسالی که گذشت

نوروز ۱۳۹۲ www.aftana.ir

ویژه نامه خبری افتانا

بررسی وضعیت امنیت فضای تولید و تبادل اطلاعات در سال ۱۳۹۱ در گفتگو با کارشناسان

بسم الله الرحمن الرحیم

امنیت سایبری، دکترین یا استراتژی


علیرضا صالحی

وقوع حملات متعدد به زیرساخت‌های سایبری کشورمان و آشکار شدن نقش کشورهای غربی در سازماندهی حملاتی نظیر استاکس نت، جای هیچگونه شبهه‌ای در مورد لزوم تدوین استراتژی یا راهبرد امنیت سایبری برای کشور باقی نگذاشته است.
اما آیا ما در این زمینه به استراتژی نیازمندیم یا باید فراتر از آن، به یک دکترین در خصوص امنیت در فضای سایبر بیندیشیم؟

در تعریف آمده است که دکترین اصول عقیده یا قواعد بنیادینی است که هدایت کننده اقدام در پشتیبانی از سیاست‌ها و برنامه‌ها در جهت تامین اهداف بوده و به کاربردن آن‌ها مستلزم درک مقتضیات و تصمیم‌گیری صحیح و منطقی می‌باشد. به عبارت دیگر اصول یک نظام فکری یا سیاست و خط مشی را دکترین می‌گویند. در کنار آن، مفهوم استراتژی وجود دارد که فن و علم توسعه و به کارگیری قدرت به منظور پشتیبانی از سیاست‌ها و افزایش احتمال دستیابی به نتایج مطلوب و پیروزمندانه است.

نگاهی به چندگانگی مراکز تصمیم‌گیری در فضای سایبر که از تعدد گذشته و به مرز وفور (!) رسیده است، نشان می‌دهد که آنچه که فعلا در کشورمان در خصوص دفاع سایبری وجود دارد، نه تنها از جنس دکترین نیست؛ بلکه از استراتژی و راهبرد نیز فاصله بسیاری دارد و بیشتر به راهکارها و تاکتیک‌هایی کوتاه مدت می‌ماند.
تاکتیک‌هایی که سازمان‌های مختلف هرکدام، به فراخور توان، بودجه، ماموریت و اضطرار، با اجرای آن سعی می‌کنند که گرهی از مشکلات باز کنند و نقشی در مقابله با تهدیدات سایبری ایفا نمایند.

در دیگر سو، ایجاد ساختارهای دفاع سایبری در بیش از سی و دو کشور جهان و اهتمام بیش از یکصد کشور جهان به انجام مطالعات اساسی در این زمینه و توجه جدی جامعه جهانی به موضوع جنگ سایبری و هشدارهای سازمان ملل در رابطه با خطرات حملات این چنینی، نشان می‌دهد که فصل نوینی در این زمینه رقم خورده است.
هنگامی که دولت ایالات متحده، رسما در مقابله با حمله سایبری، حمله نظامی را جایز اعلام می‌کند و دولت روسیه در گامی فراتر، حق حمله هسته‌ای در جواب حمله سایبری/اطلاعاتی را مجاز می‌شمارد، راهبرد کلان ما در این زمینه چیست؟

آیا می‌توان همچنان بدون توجه به مولفه‌های فضای سایبری، بدون مشارکت دادن همه ذینفعان، فارغ از توجه به نقش انکار ناپذیر جامعه کاربران، به دور از لزوم رصدکردن مستمر اتفاقات فضای مجازی و خلاصه بدون وجود یک نگاه کلان نگر و مبتنی بر قواعد بنیادینی از جنس دکترین، در فضای سایبر زیست؟
مطمئنا آنانی که در حال برنامه‌ریزی برای آسیب‌رسانی به حریم‌های مجازی کشورمان هستند، به خوبی این ضعف بزرگ را می‌شناسند و به آن واقفند. اما با تشکیل شورای عالی فضای مجازی، که نهادی بالادستی برای توجه به این فضا است، می‌توان به داشتن دیدگاهی کل نگر امیدوار بود.

* این یادداشت قبلاً در مرجع امنیت (۱۳۹۱) منتشر شده و افتانا آن را بازنشر می‌نماید.

تجارت امن

توانایی دفاع سایبری از الزامات حفظ مرزهای کشور است

در شرایطی که کشور با تهدیدهای متعددی در زمینه امنیت اطلاعات مواجه است، استفاده از ابزارها و فناوری‌های نوین و تولید، نصب و راه‌اندازی محصولات بومی در حراست از فضای سایبری کشور نقش به سزایی خواهد داشت، و نقش دولت در گسترش این فناوری‌ها بر کسی پوشیده نیست در این خصوص با مهندس حمیدبابادی‌نیا، مدیرعامل شرکت گیلاس کامپیوتر به گفتگو نشستیم که شرح آن را در ادامه می‌خوانید:

مهم‌ترین رویداد امنیتی حوزه افتا از دید شما در سال ۹۱ چیست؟

به عقیده من مهم‌ترین رویداد سال ایجاد تعامل مثبت بین سازمان فناوری اطلاعات خصوصا معاونت امنیت این سازمان با کمیسیون افتا سازمان نظام‌صنفی رایانه‌ای کشور از طریق برگزاری جلسه گفتگو بوده است که پل ارتباطی میان بخش خصوصی و بخش دولتی ایجاد کرد. این جلسه پل ارتباطی بود میان سازمان نظام صنفی رایانه و سازمان فناوری اطلاعات که نیازهای بخش خصوصی به سازمان فناوری اطلاعات و نیازهای بخش دولتی به بخش خصوصی منتقل شد.
به طور قطع این دست تعاملات بین بخش خصوصی و بخش دولتی باعث رشد صنعت فناوری اطلاعات خصوصا در بحث امنیت خواهد شد.

با توجه به اینکه کشور ما آماج حملات سایبری است، تحلیل شما از این رویدادها چیست و آینده را چطور ارزیابی می‌کنید؟

با توجه به موقعیت خاص ایران در جامعه جهانی و سیاست‌هایی که در خصوص تعاملات خود با دنیای خارج اتخاذ کرده است در معرض تهدیدهای مختلفی قرار دارد که عرصه ارتباطات نیز از این قاعده مستثنی نیست.
رشد فناوری‌های امنیتی در فضای مجازی نیز یکی از انواع حفظ و حراست مرزها است، افزایش تهدیدات باعث توجه بیشتر کارشناسان و متخصصان این رشته در جهت ارتقاء دانش مورد نیاز در زمینه تولید و نصب و راه اندازی این فناوری و جلوگیری از بروز صدمات مخرب در این حوزه شده و صدمات این بخش را به حداقل رسانده است. با این تفاسیر مطمئنا آینده روشنی پیش روی پیشرفت فناوری‌های امنیتی خواهد بود. لازم به ذکر است که دستیابی به فناوری‌های پیشرفته بدون حمایت بخش دولتی از بخش خصوصی و شرکت‌های تحقیقاتی حاصل نخواهد شد.
در حال حاضرکشور ما از نظر تولید تجهیزات امنیتی و فایروال در ابتدای راه است و لازم است که بر روی افزایش تنوع محصولات و ارتقاء آن‌ها تمرکز بیشتری داشته باشد. البته هم اکنون ایران تنها کشور حوزه خلیج فارس است که توانایی تولید، نصب و راه اندازی تجهیزات امنیتی را دارا است.

رویکرد بخش دولتی نسبت به حضور بخش خصوصی در حفظ امنیت سایبری را چطور ارزیابی می‌کنید؟

امنیت پیرامونی معطوف به ارتباط سیستم‌ها با دنیای خارج است در مواقعی که تهدیدی از سوی دنیای خارج مرزهای سایبری را تهدید می‌کند، بخش دولتی در مقابل آن سدهایی ایجاد می‌کند اما زمانی که رخنه ای در مسیر ورود وجود داشته باشد پس از ورود ویروس‌ها یا بدافزارها به فضای داخلی کشور حفظ امنیت در حیطه وظایف بخش خصوصی است تا با نصب فایر وال‌ها و درگاه‌ها شبکه اطلاعاتی سازمان‌های کشور را محافظت کنند بنابر این لازم است که بخش دولتی در این خصوص از بخش خصوصی حمایت کند.

نقش دولت در توانمندسازی بخش خصوصی در تولید محصولات بومی چیست؟

بخش دولتی و مشخصا سازمان فناوری اطلاعات می‌تواند از طریق برگزاری مناقصات، تعریف و ارائه پروژه‌ها و دعوت از بخش خصوصی برای شرکت در تحقیقات و تجاری کردن پروژه‌ها با ایجاد فضای رقابتی در پیشرفت فناوری‌ها سهیم شود. همچنین از طریق ارائه تسهیلات مالی بخش خصوصی را در جهت تولید محصولات بومی یاری کند.
تاکنون فعالیت دولت در توانمندسازی بخش خصوصی هدفمند نبوده است بنابراین لازم است برنامه‌ریزی‌هایی در این زمینه صورت گیرد و با برآوردهای کارشناسی شده تحقیقاتی انجام شود که دولت خود خریدار آن‌ها باشد.

عامل اساسی آسیب‌پذیری کشور در بحث امنیت را درچه زمینه‌ای می‌بینید؟ و برای رفع آن چه راهکارهای را پیشنهاد می‌کنید؟

در حال حاضر تجهیزات امنیتی سازمان‌ها و ارگان‌های بزرگ کشور از بازدارندگی کافی برخوردار نیستند و در سیستم‌های آن‌ها رخنه‌هایی وجود دارد. لازم است با استانداردسازی تجهیزات و الزام سازمان‌ها و ارگان‌ها به داشتن تجهیزات ISMS، بازنگری دوره‌ای این تجهیزات و انجام آزمون‌های نفوذ، جهت شناسایی راه‌های نفوذ احتمالی ضریب امنیتی سازمان‌ها را افزایش دهیم. با ایجاد الزام در این زمینه نه تنها در حفظ اطلاعات و منابع کشور گام بزرگی بر خواهیم داشت بلکه از هدر رفت منابع نیز جلوگیری خواهد شد.

با توجه به اظهارات غرب در خصوص ارتش سایبری ایران، دیدگاه شما چیست؟ وجود ارتش سایبری تا چه اندازه در کنترل این گونه حملات کمک می‌کند؟ آیا قائل به وجود ارتش سایبری هستید یا افزایش توان به منظور بازدارندگی را توصیه می‌کنید؟

همان گونه که با قائل شدن به مرزهای فیریکی نیاز به وجود ارتش به وجود می‌آید، در فضای سایبری نیز مرزهایی وجود دارد که با پذیرفتن وجود این مرزها نیاز به وجود ارتشی برای مقابله با خطرات احتمالی یک الزام است. همچنین که کشورهایی که در حال حاضر با خطر حملات سایبری مواجه نیستند نیز در حال بالا بردن ضریب امنیتی در فضای سایبری خود هستند.
همچنین با بالابردن دانش فنی فناوری اطلاعات در حوزه امنیت و ایجاد امنیت در زیرساخت‌های کشور و با بهره‌گیری از حداقل تجهیزات امنیتی می‌توانیم با ایجاد بازدارندگی از تاثیر مخرب حملات سایبری بکاهیم.

تجارت امن

افتای ایرانی در سالی که گذشت
ویژه‌نامه نوروزی افتانا
اسفند ۱۳۹۱/ فروردین ۱۳۹۲

سردبیر: علیرضا صالحی
گفتگوها: مریم اصلان زاده، فرزانه دهرویه، نشاط کردرستمی
گرافیک: نیلوفر فروغی
با سپاس از: سازمان پدافند غیرعامل، سازمان فناوری اطلاعات ایران، بانک مرکزی جمهوری اسلامی ایران و شرکت‌های گیلاس کامپیوتر، تجارت‌امن، قاصدک سامانه، تجارت الکترونیک ایرانیان (ایدکو)، ایمن رایانه پندار، کارنما رایانه، آروین رایان ارتباط، کهکشان نور، پویه، مهران رایانه، اینفوامن، دمسان رایانه و رایان سامانه آرکا.

info@aftana.ir تلفن: ۸۸۵۱۹۱۸۲

آگاهی‌رسانی در امنیت؛ یک قدم به جلو

با فراگیر شدن اینترنت و استفاده از آن برای انجام کارهای روزمره در خانه و سازمان‌ها، نفوذگران و هکرها نیز بیش از گذشته به فکر سوءاستفاده از اطلاعات و سرقت آن‌ها افتاده‌اند. این روزها هکرها علاوه بر استفاده از روش‌های قدیمی هک به روش‌های جدیدی که مبتنی بر مهندسی اجتماعی هستند نیز روی آورده‌اند. به طوریکه سعی می‌کنند با استفاده از تکنیک‌های روانشناسی بر ذهن قربانیان تاثیر گذاشته و اطلاعات مورد نظرشان را به سرقت ببرند.

نفوذگران سعی می‌کنند کاربران را فریب دهند تا آن‌ها با دست خودشان اطلاعات مهم و حساس را لو دهند. در چنین شرایطی شاید بتوان گفت در اولین قدم تنها کاربران آگاه و آموزش دیده هستند که می‌توانند جلوی سودجویی هکرها را بگیرند. محمد مبصری قائم مقام شرکت کامگارد و مدیر عامل شرکت تجارت امن در گفت و گو با افتانا در این راستا گسترش بیش از پیش ویروس‌هایی نظیر فلیم و مینی فلیم، نتیجه ناآگاهی کاربرانی می‌داند که بدون توجه به زوایای مهم امنیت و حفظ آن در فضای مجازی، باعث درز اطلاعات مهم و حساس کشور می‌شوند.

نیاز کشور؛ معماری امنیت

به اعتقاد مبصری مهم‌ترین رویداد سال ۹۱ در حوزه افتا حمله ویروس فلیم به کشور بود که به صورت نامحسوس بین سیستم‌های قربانیان حرکت می‌کنند تا به سیستم هدف که ممکن است مالی یا صنعتی باشد رسیده و آسیب نهایی را وارد و یا اطلاعات لازم را سرقت کنند. وی معروف‌ترین نسخه‌های این سری از بدافزارها را استاکس نت و دوکو می‌داند و بر افزایش این نوع حملات سایبری در تمام دنیا تاکید می‌کند و می‌گوید: «با توجه به موقعیت خاص کشور ما، طی سال‌های اخیر شاهد افزایش روزافزون ویروس‌های مخرب و حملات سایبری با هدف ضربه زدن به کشور و سرقت اطلاعات بوده‌ایم. از این رو انتظار می‌رود مسئولان کشور استراتژی‌های گذشته را توسعه داده و معماری امنیت کشور را با هوشمندی بیشتری طراحی کنند.»

به گفته مدیرعامل شرکت تجارت امن این شرایط در حالیست که متاسفانه به دلیل بروز برخی مشکلات اقتصادی و افزایش قیمت تجهیزات امنیتی، برخی سازمان‌های دولتی و یا شرکت‌های خصوصی از تجهیزات یا نرم‌افزارهای امنیتی قفل شکسته استفاده می‌کنند در چنین شرایطی و در نتیجه چنین اقدامی به سازمان‌های دولتی و زیر ساخت‌های امنیت کشور آسیب پذیر وارد شده و اطلاعات کشور به بیرون درز می‌کند. وی در این مورد ادامه می‌دهد: «البته باید این نکته را نیز مدنظر قرار داد که مدتی است برخی سازمان‌های دولتی رو به استفاده از تجهیزات کاملا بومی آورده‌اند که اگرچه استفاده از این ابزار مزایایی دارد اما در جای خود و به دلیل اینکه هنوز به بلوغ کامل نرسیده‌اند، مشکلاتی را هم به وجود خواهند آورد.»

مدیرعامل شرکت تجارت امن رفع این مشکل و تولید محصولات بومی را در گرو در اختیار داشتن بودجه و امکانات می‌داند و در این مورد یادآوری می‌کند: «اختصاص بودجه و امکاناتی که بتوانند در ضمن آموزش تخصص به صورت موازی از تکنولوژی تجهیزات مناسب خارجی استفاده کنند در نهایت باعث افزایش کارایی تجهیزات بومی خواهند شد.» مبصری همچنین امنیت لایه به لایه با تجهیزات خارجی و بومی به صورت همزمان را نیز راهکار مناسبی در ارائه محصولات بومی با کیفیت و همچنین کارا می‌داند.

آموزش، آموزش، آموزش

قائم مقام شرکت کامگارد علاوه بر عدم وجود محصولات بومی کارا، عدم آگاهی کافی کاربران نسبت به مقوله امنیت را نیز یکی از جدی‌ترین آسیب‌پذیری‌های کشور در این حوزه عنوان می‌کند. وی در این مورد می‌گوید: «متاسفانه اکثر کاربرانی که در سازمان‌های بزرگ و مهم کشور مشغول به فعالیت هستند، چندان از مسائل فنی و اهمیت امنیت سیستم‌ها آگاهی ندارند.» مبصری در نهایت در مورد روند و چگونگی حل این مشکل می‌گوید: «عدم آگاهی و عدم تسلط کارمندانی که به هر شکل در سازمان‌هایی که زیرساخت‌های حیاتی کشور را اداره می‌کنند، مشغول به کار هستند، فقط از طریق آموزش علوم روز در این زمینه امکان‌پذیر خواهد بود.»

حمـــایت از بخـــش خصوصـــی لازمـــه حفظ امنیت ســـایبـــری

با نگاهـی دقیق به وضعیت امنیت سایبـری کشـور و تهدیداتی که از هر سو کشور ما را تهدید می‌کند توجه بیشتر به تولید محصولات بومی برای جلوگیری از بروز خسارات احتمالی و کاهش ضریب خطا در حـوزه امنیت امری مهم و ناگزیر می‌نماید که نیازمنـد حمایت مسئولین دولتـی از متخصصـان داخلـی است در ایـن خصوص گفتگویـی داشتیم با کاظم قنبـری، مدیـرعامل شرکت قاصدک که در ادامـه می‌خوانید.

مهم‌تـرین رویداد امنیتی حوزه افتـا از دید شمـا در سال ۹۱ چیست؟

به عقیده من مهم‌ترین رویداد حوزه افتا در سال جاری، اخبار مربوط به استاکس‌نت و فلیم و مسائل امنیتی مربوط به آن بوده است زیرا پس از این رویداد سازمان‌های کشور نسبت به امنیت فضای مجازی خود هوشیارتر شده و امنیت شبکه برای آن‌ها به مسئله مهمی تبدیل شد. مسئله دیگر اینکه سازمان‌های دولتی متوجه شدند محصولات خارجی لزوما معتبر نیستند و فضایی برای فعـالیت بیشتر بخش خصوصی در حوزه امنیت فراهم شد.

با توجه به اینکه کشور ما آماج حملات سایبـری است، تحلیل شما از این رویدادها چیست و آینده را چطور ارزیابی می‌کنید؟

زمانی که بپذیریم دشمنی وجود دارد و بروز انواع حملات رفتار طبیعی دشمن است لازم می‌دانیم تمهیداتی برای مقابله با حملات دشمن از جهات مختلف بیندیشیم حملات سایبری اخیر باعث شد تا مسئولین کشور با هوشیاری بیشتری با مسئله امنیت فضای سایبری برخورد کنند و نیاز به استفاده از محصولات بومی را در این حوزه احساس کنند بهترین راه مقابله با دشمن خارجی بهره‌منـدی از امکانات داخلی بهتـرین راه است. علاوه بر آن باید در نظـر داشته باشیم کـه تنها راه مقابله جلوگیـری از بروز حملات از سوی دشمن نیست و لازم است در این راستـا به مقابله به مثل نیز بپردازیم تا بتوانیـم نیروی خود را تقـویت کنیم.

رویکرد بخش دولتی نسبت به حضور بخش خصوصی در حفظ امنیت سایبری کشـور چیست؟

علیرغم این که در چند سال اخیر توانمندی‌های بخش خصوصی رشد مناسبی داشته و در مقایسه با شرکت‌های خارجی قابل اعتمادتر است بخش دولتی هنوز اعتماد لازم را به این بخش ندارد این در حالی است که با حمایت از بخش خصوصی و متخصصان داخلی در جهت رشد و افزایش دانش و توانمندی‌ها بیشتر می‌توان به حفظ امنیت مرزهای سایبری کشور امید داشت، زیرا بخش خصوصی داخلی در بسیاری از جهات در دسترس تر و قابل اعتمادتر از یک شرکت خارجی است در حالی که امکان فروش اطلاعات از سوی یک شرکت خارجی بیشتر است. علاوه بر این یک محصول بومی متناسب با نیازهای داخلی طراحی می‌شود و مسلما خرید و استفاده از آن هزینه کمتری را بر سازمان‌ها تحمیل خواهد کرد پس حمایت از بخش خصوصی لازمه حفظ امنیت است. در حالی که یک محصول خارجی در بسیاری از موارد متناسب با نیازهای داخلی نیست و هزینه بالایی در بر دارد.

نقش دولـت در تـوانمندسـازی بخـش خصوصـی در تولیـد محصولات بومی چیست؟

محصولات داخلی هم مانند تمام محصولات خارجی از نقطه صفر شروع کرده‌اند و هنوز در ابتدای راه هستند و همچنان که در محصولات خارجی پس از گذشت سال‌ها خطاها و اشکالاتی بروز می‌کند در محصولات داخلی نیز عاری از خطا نخواهند بود اما نکته مهم این است که تا زمانی که محصولات بومی مورد استفاده قرار نگیرند ایرادات و نیازهای آن‌ها شناخته نخواهد شد و امکان رفع آن‌ها میسر نمی‌شود. علاوه بر آن تولید محصولات بومی نیازمند حمایت‌های مادی و معنوی بخش دولتی است زیرا در شرایط اقتصادی فعلی انجام تحقیقات با بودجه شخصی ریسک بزرگی برای شرکت‌های خصوصی خواهد بود و تامین منابع مالی یکی از مشکلاتی است که سد راه انجام تحقیقات در این زمینه شده است. حمایت‌های معنوی نیز باید به گونه ای باشد که حمایت از شرکتی که دارای رانت است باعث ضایع شدن حق دیگران و برهم خوردن بازار نشود و همچنین سازمان‌های داخلی ملزم به خرید محصولات داخلی شوند.

عامل اسـاسی آسیب‌پذیری کشـور در بحث امنیت را در چـه زمینـه‌ای می‌بینید؟ و برای رفع آن چه راهکـاری را پیشنهـاد می‌کنید؟

اولا مسئولین سازمان‌ها در بحث هزینه‌های امنیتی توجیه نیستند و در بودجه بندی‌ها به بحث امنیت توجه نمی‌کنند این امر باعث می‌شود در صورت بروز خسارت دهها برابر هزینه بر آن سازمان تحمیل شود، بنابراین لازم است در بودجه‌بندی شرکت‌ها و سازمان‌های دولتی حفظ امنیت مورد توجه قرار گیرد و بودجه‌هایی جهت حفظ امنیت تعیین شود تا از بروز خسارات احتمالی جلوگیری به عمل آید.

ثانیا مسئولین IT سازمان‌ها نیز از دانش فنی کافی در حوزه امنیت برخوردار نیستند و معمولا به محصولات خارجی بیشتر اعتماد می‌کنند و در مورد محصولات داخلی نیز بدون تحقیق و آزمایش اقدام به خرید می‌کنند که این امر به زیان سازمان‌ها خواهد بود. لازم است که سازمان‌های دولتی اقدام به به‌کارگیری و تربیت نیروهای متخصص در این زمینه نمـایند.

با توجه به اظهـارات غرب در خصوص ارتش سایبـری ایـران، دیدگاه شما چیست؟ وجود ارتش سایبری تا چه اندازه در کنترل این گونه حملات کمک می‌کند؟ آیا قائل به وجود ارتش سایبری هستید یا افزایش توان به منظور بازدارندگی را توصیه می‌کنیـد؟

این مسئله که کشور ما دارای دشمن است امری کاملا واضح است و وجود دشمن در فضای سایبری نیز با توجه به استراتژی آن‌ها برای صدمه وارد کردن به کشور امری روشن است بنابراین داشتن ارتش سایبری کاملا ضروری است زیرا در فضای سایبری خطرات بیشتری وجود دارد و تهدیدات و حجم خسارات این حوزه قابل پیش‌بینی نیست. علاوه بر آن در فضای مجازی در روز چندین ابزار خطرناک حمله و تخریب تولید می‌شود که اثر بخشی بالایی دارند بنابراین دارا بودن ارتش سایبری برای مقابله با این حملات حق مسلم هر کشوری است. همچنین افزایش توان برای مقابله به مثل و بازدارندگی با افزایش توانمندی‌ها و رشد دانش فنی داخلی امری است که باید بسیار مورد توجه قرار گیرد.

هر بانکی مسئول تامین امنیت کاربرانش است

درگفت وگو با مدیرکل فناوری اطلاعات و ارتباطات بانک مرکزی:

بانک مرکزی جمهوری اسلامی ایران به منظور حفظ و ارتقای امنیت نظام پرداخت، بانکداری الکترونیکی و مواجهه درست با تهدیدات درونی و بیرونی نظام بانکی کشور، مرکز کنترل امنیت شبکه و فوریت‌های بانکی را با عنوان «کاشف» راه‌اندازی کرده است.

این مرکز، موظف به مدیریت رخدادهای امنیتی در فضای سایبری بانکی کشور است که وظیفه جمع‌آوری و اشتراک‌گذاری اطلاعات و هماهنگی بین بانک‌ها را در مواقع بروز رخدادهای امنیتی و بحران‌های سایبری بر عهده دارد.

در همین راستا افتانا طی یک گفت و گوی اختصاصی با ناصر حکیمی مدیرکل فناوری اطلاعات و ارتباطات بانک مرکزی به بررسی تمهیدات بانک مرکزی در مواجهه با تهدیدات سایبری پرداخته داده است که در ادامه می‌خوانید.

ناصر حکیمی در گفت و گو با افتانا هدف از ایجاد مرکز کاشف را تمرکز بر آن دسته از رخدادهای امنیتی دانست که در خارج و یا داخل شبکه بانکی رخ می‌دهد. وی در این مورد گفت: «مرکز کاشف سعی دارد کلیه رخدادهای امنیتی را در جایی متمرکز جمع‌آوری کند تا امکان تحلیل، اثرسنجی و در نهایت ارائه سریع دستورالعمل در ارتباط با آن رویداد فراهم شود.»

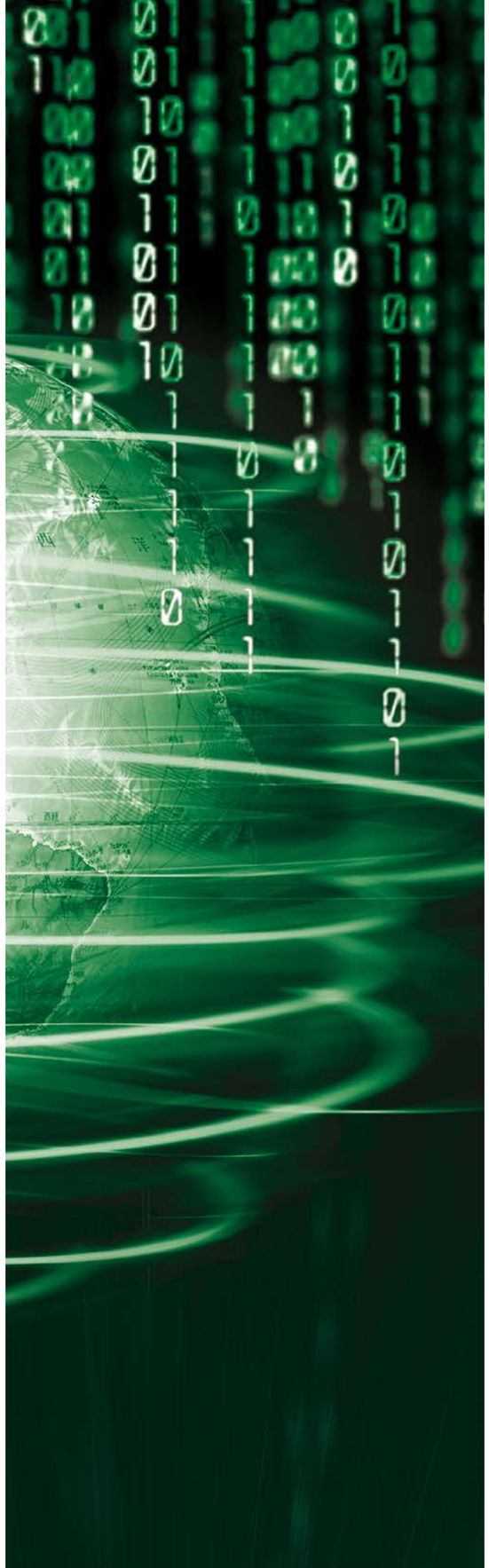
حکیمی کاشف را یک مرکز Cert دانست که قبل از هر چیز وظیفه اطلاع‌رسانی و همچنین جمع آوری اطلاعات در ارتباط با رویدادهای امنیتی را برعهده دارد. وی در این مورد تصریح کرد: «در واقع این مرکز به بررسی تهدیدات پس از شناسایی یک حمله در داخل و همچنین بررسی رخدادهای امنیتی در سطح بین‌المللی می‌پردازد. چرا که ممکن است تهدیداتی در سطح جهانی وجود داشته باشد که به مرور زمان شبکه بانکی کشور را نیز درگیر کند. کاشف با تحلیل این تهدیدات قبل از وقوع حادثه، هشدارهای لازم را به شبکه بانکی ابلاغ می‌کند.»

مدیر کل فناوری اطلاعات بانک مرکزی افزایش حضور کاربران در فضای مجازی و انجام عملیات بانکی بر بستر اینترنت، را نیازمند توجه بیشتر بانک‌ها به مقوله تامین امنیت دانست و گفت: «اگرچه تاکنون نقص جدی امنیتی در سیستم‌های بانکی وجود نداشته و هیچ نفوذی به سایت بانک‌ها باعث لو رفتن اطلاعات مالی کاربران نشده است، اما بانک‌ها اولین لایه در مقابله با نفوذ غیرمجاز هکرها به شبکه بانکی خود هستند.»

به گفته حکیمی بانک‌ها همانطور که مسئول حفظ امنیت شعبه، ماشین حمل پول و یا هر چیز فیزیکی دیگری هستند، موظفند امنیت خود در فضای مجازی را نیز حفظ کنند و در این راستا بانک مرکزی مسئولیتی در قبال ضررهای ناشی از بی توجهی بانک‌ها در این خصوص نخواهد داشت.

وی در این مورد یادآور شد: «بانک مرکزی در این خصوص تنها دستورالعمل‌هایی را به بانک‌ها ابلاغ می‌کند و بانک‌ها موظف به اجرای آن‌ها هستند و چنانچه از آن تخطی کنند، باید به بانک مرکزی پاسخگو باشند.»

وی در خاتمه گفت و گوی خود با افتانا با اشاره به فراگیر بودن و قابل سرایت بودن تهدیدات فضای سایبر گفت: «هدف بانک مرکزی جمع آوری تهدیدات موجود در فضای مجازی و به اشتراک‌گذاری آن‌ها بین مسئولان بانکی است تا میزان ریسک و خطرپذیری شبکه بانکی کشور را به حداقل ممکن برساند.»



ارتش سایبری، بعد جدید قدرت

آنهایی که سر و کارشان با امنیت و ابزارهای امنیتی است، جور دیگری فضای مجازی را می‌بینند و امنیت برایشان رنگ و بوی دیگری دارد. برای این متخصصان امنیتی، حضور و ورود تبهکاران و بزهکاران سایبری بدترین اتفاقی است که می‌تواند در فضای سایبر بیفتد. به همین دلیل هم است که اگر از آن‌ها بپرسید بدترین اتفاق سال ۹۱ چه بود احتمالا از حمله ویروس‌ها و دزدیده شدن اطلاعات کاربران یاد می‌کنند. سینا بقایی مدیرعامل شرکت ایدکو هم از همان دسته متخصصانی است که حفظ امنیت کاربران در فضای مجازی را تا سر حد نان شب واجب می‌داند.
در ادامه گفت و گوی افتانا با وی را بخوانید.

مهم‌ترین رویداد امنیتی حوزه افتا در سال ۹۱ از دیدگاه شما چیست؟

به اعتقاد من حمله ویروس فلیم به وزارت نفت و سازمان‌های متبوعش به دلیل طولانی بودن زمان شناسایی آن از مهم‌ترین اتفاقات امنیتی سال ۹۱ بود. شاید بتوان گفت تفاوت در نوع طراحی این ویروس خسارت‌های زیادی را به بار آورد. در واقع ویروس فلیم به دلیل تفاوت در ساختار طراحی و همچنین حجم خسارتی که به بار آورد، نسل جدیدی از ویروس‌ها بود.

با توجه به اینکه کشور ما آماج حملات سایبری است، تحلیل شما از این رویدادها چیست و آینده را چطور ارزیابی می‌کنید؟

هرچه میزان وابستگی افراد به چیزی بیشتر شود، خطرات و آسیب‌پذیری‌های آن، نیز بیشتر می‌شود. به عنوان مثال، ویندوز که کاربران زیادی دارد، همواره مورد حمله بیشتر بدافزارها قرار گرفته است. این مسئله که تا چه میزان به ابزارهای تکنولوژی و صنعت IT که کلیه فعالیت‌های اقتصادی، بازرگانی و تولیدی را درگیر خود کرده است، وابسته هستیم ما را با خطرات بیشتری در این حوزه مواجه کرده و خواهد کرد. این قضیه در مورد کشورها نیز صادق است. طی سال‌های اخیر سیاست‌های هسته‌ای ایران که همگام با جامعه جهانی نبود، سبب شد تا سایر کشورها به جای لشگرکشی به کشور برای مقابله با این سیاست‌ها ترجیح بدهند از ابزارهای مخصوص فضای مجازی برای دریافت اطلاعات بهره ببرند. البته باید این نکته را هم مدنظر داشته باشیم که این آسیب‌پذیری‌ها تنها مربوط به کشور ما نیست. به طوریکه هر روز در اخبار شاهد ظهور و بروز ویروس‌های تخریب‌گر به سازمان‌های اروپایی و امریکایی هستیم.

رویکرد بخش دولتی نسبت به حضور بخش خصوصی در حفظ امنیت سایبری را چطور ارزیابی می‌کنید؟

به دلیل اینکه اکثر شرکت‌های خصوصی فعال در حوزه امنیت نماینده شرکت‌های خارجی هستند و تولید داخلی چندانی در زمینه تامین امنیت وجود ندارد، بدنه دولتی اعتماد و اطمینان چندانی به محصولات خارجی ندارند و همواره این نگرانی در بین آن‌ها وجود دارد که احتمال اینکه این شرکت‌های امنیتی تولید کننده محصولات غیر بومی، قصد خروج اطلاعات آن‌ها را دارند. نتیجه چنین تفکری عدم اعتماد به محصول خارجی و همچنین عدم دخالت بخش خصوصی در تصمیمات کلان کشوری می‌شود.

با این اوصاف شما راه حل را در تولید محصولات بومی توسط بخش خصوصی می‌بینید. در این صورت دولت چه نقشی در توانمندسازی بخش خصوصی می‌تواند داشته باشد؟

اگر واقعاً این نگرانی از سوی دولتی‌ها وجود دارد که با استفاده از محصول خارجی اطلاعات آن‌ها درز پیدا می‌کند، پس باید سرمایه‌گذاری‌های قابل قبولی در این حوزه فراهم شود تا به مرور زمان محصول داخلی که همگام با استانداردهای جهانی در حال رشد است، جایگزین محصول خارجی شود. چنین اتفاقی تنها با تخصیص بودجه و همچنین یک کار گروهی امکان‌پذیر خواهد شد. زمانی من پیشنهاد تولید یک ضدبدافزار بومی را دادم که در کنار یک ضدبدافزار خارجی کار کند. در این شرایط و به مرور زمان ضدبدافزار داخلی رفتار خود را تطبیق داده و نقاط ضعف خود را اصلاح خواهد کرد.

با توجه به اظهارات غرب در خصوص ارتش سایبری، لطفاً دیدگاه خود را در این خصوص بفرمائید آیا وجود چنین ارتشی به کنترل حملات کمک می‌کند؟

با توجه به اینکه سایر کشورها نیز چنین رویکردی را مد نظر قرار داده و آن را توسعه می‌دهند، وجود چنین ارتشی می‌تواند تا حدی خوب باشد. در واقع ارتش سایبری به عنوان بعد جدیدی از ارتش‌ها وارد عمل شده و از مرزهای مجازی محافظت می‌کنند. البته به نظر من بهتر است ارتش سایبری را محدود به مقابله با حملات سایر کشورها نکنیم و از وجود چنین ارتشی برای جلوگیری از ورود تبهکاران و بزرگکاران داخلی و خارجی به محدوده مجازی کشور بهره ببریم.

دانش و تجربه بومی، دروازه ورود به امنیت

اگـرچه در گذشتـه‌ای نـه چنـدان دور افراد با مهارت‌هـای فردی بالا به صورت انفـرادی و با اهـداف مختلف اقـدام به نفوذ و هک سایت‌هـا می‌کردند، اما در دنیای امـروز هستند کشورهـایی که این افراد را شناسایی کرده و در غـالب یک ارتش سایبـری سازماندهی شده به خدمت می‌گیرند. وجود چنیـن ارتشی در کشورهـا قطعـاً دیگـر نـه برای اهـداف فردی نفوذگران بلکـه با هدف رسیـدن به مقاصد کلان ملـی صورت می‌گیـرد.

رضـا پرسـتـه مدیر بازاریابی و فروش شرکت ایمن رایـانه پنـدار نماینده انحصـاری محصولات امنیتی پاندا در ایـران، در گفت و گو با افتانـا داشتن ارتش سایبری ایـران را اگرچـه مایه مباهات می‌داند امـا معتقد است این ارتش بایـد فـارغ از سیاست گذاری‌هـای ملی، از تـوان و مهارت خود در طراحی و پیـاده‌سازی لایه‌های مختلف حفـاظتی و امنیتی برای شبکه‌هـای رایانـه‌ای داخل کشـور بهره ببرد.

ایـران: مقصد خوب جنگ سایبـری

مدیر بازاریـابی و فروش شرکت ایمن رایـانه پنـدار با وجود آنکه ماننـد بسیـاری دیگر از متخصصان حوزه امنیت هجوم کد مخـرب فلیـم را مهم‌تـرین رویـداد سال ۹۱ در حوزه افتـا می‌دانـد، اما معتقد است اگرچـه این ویروس تبعات بدی برای کشور داشت اما موجب افـزایش اهمیت سازمان‌هـا به مقولـه امنیت اطلاعـات، جدی گرفتن پـروژه سیستم عامل و ضدبدافزار بومی، کاهش نسبی اعتمـاد به ضدبدافزارهای خارجی و ضرورت سـاماندهی آن‌هـا در کشور نیز شده است.

به اعتقاد وی از آنجـا که ایـران در منطقه استراتژیک خاورمیـانه واقع شده است همـواره با انـواع مختلف تهدیدها و توطئه‌هـا روبرو بـوده است و هم اکنون نیز در جنگ سایبـری یکی از کشورهای مورد توجه است. پرسـتـه در این مـورد توضیح می‌دهد: «بـه لحـاظ کم هزینه‌تـر بودن جنگ سایبـری، اکنـون کشورهـای قدرت طلب جهـان ماننـد امریکـا و اسرائیـل سعی دارند تـا از این طـریق به اهـداف خود بـرسند.» وی ادامه می‌دهد: «در چنین شرایطـی بعیـد به نظر می‌رسـد حجـم ایـن حملات در آینـده کاهش پیدا کند. مگر آنکه کشورهـای متخـاصم روش جدیدتری برای دستیابی به مقاصد خود پیداکننـد.»

مدیر بازاریابی و فـروش شرکت ایمن رایـانه پنـدار در چنین شرایطی وظیفه بخش دولتـی و خصوصی را پیشگیـری هوشمندانـه حملات سایبـری می‌دانـد. به اعتقـاد وی این اتفـاق تنهـا از طـریق به کارگیـری لایه‌هـای مختلف امنیتی در شبکه‌هـای رایـانه‌ای و حتی ایـزوله کـردن برخی سیستم‌های حاوی اطلاعات بسیـار مهـم و محرمانه صورت می‌پـذیرد. پـرسته در این خصوص اضافه می‌کند: «البته لـزوم توجـه به دانش و تجربه بومی در موفقیت پیشگیـری از اینگونه نفوذهـا امر بسیـار مهمی است.»

تعـاملی که باید بـاشد، امـا نیست...

رضا پرسـتـه در ادامه گفت و گـوی خـود با افتانـا به عدم اعتمـاد بخش دولتـی نسبت به توانمندی‌هـای بخش خصـوصی اشـاره می‌کنـد. به اعتقـاد وی عدم تعامل و اعتمـاد دولت به بخش خصوصی عـامل اصلـی انزوای این بخش است که جلوی رشد را از آن‌هـا می‌گیرد. چراکه توان مـالی بخش خصوصی محدودتـر از آن است که بتوانـد صرف تحقیقات مختلف در حـوزه امنیت اطلاعـات و تولید نرم‌افزارهـای بـومی شود. از این رو کمک بخش دولتـی در این حوزه اجتناب نـاپذیر است.

مدیر بازاریـابی و فروش شرکت ایمن رایـانه پنـدار نماینـده انحصـاری محصولات امنیتی پانـدا در ایـران در ادامه، تلاش دولت در تـاسیس پارک‌های علم و فنـاوری را تلاشی ناموفق در ورود به حوزه تحقیقات علوم و فنون می‌داند و در این مورد خـاطر نشـان می‌کند: «متاسفانه حلقه‌هـای زنجیـره تجربه و مهـارت بخش خصوصی، دانش مراکـز دانشگـاهی و حمایت‌های مـالی دولت نتـوانسته به هـم متصل شـود و در اغلب پروژه‌هـا کمبود حـداقل یکی از این حلقه‌هـا محسوس است.»

پرسـتـه در خـاتمه این گفت و گـو موقعیت استراتـژیک ایـران را از یک سـو و وابستگی کشور به نرم افـزارها و سخت افزارهـای خارجـی را از سوی دیگـر اصلی‌تـرین عـامل آسیب پذیـری‌هـای کشور می‌دانـد و در این مـورد می‌افـزاید: «متـاسفـانه گاهـی همین نرم‌افـزارهـا و سخت‌افـزارهـای خـارجی می‌تواننـد ماننـد سلاحی در دست بیگانگـان و راهی برای نفـوذ و حمـله به کشور مـا باشنـد. به همین دلیل و در چنین شرایطی تنهـا راه مقابلـه با چنیـن اتفـاقی ارتقـای سطح تعـامل و همکـاری حلقه‌هـای زنجیر و عـزم جدی در خودکفایی در زمینه تولید نرم‌افزارها و سخت‌افزارهای مورد نیاز کشور خواهد بود.»

تولید محصولات بومی با حذف نگاه تجاری به مبحث امنیت امکان پذیر است

تولید محصولات بومی امنیتی جهت حراست از فضای سایبری کشور امـری است نیازمنـد تولید و افـزایش دانش فنی متخصصـان این حـوزه که تنهـا با حمایت دولت از بخش خصوصی امکـان‌پذیر است، با وجـود اینکـه بخش خصوصی توان و تخصص لازم را داراست، همـواره نیازمنـد حمایت بخش دولتـی است تـا فـارغ از هرگونـه نگاه تجـاری به مسئله حساس امنیت، در تلاش برای افزایش تـوان و آگاهی خود باشد.

در ادامه گفتگوی ما با محمد علی دره شیری، مدیـرعامل شرکت کارنمـا رایـانه در خصوص نقش دولت در پیشبرد هدف خودکفایی در تولید ابزارهای امنیتی را می‌خوانیـد.

دره شیـری در پاسخ به سوال مهم‌تریـن رویـداد حـوزه افتـا در سـال ۹۱ گفت: ضعف‌هـایی که در حوزه امنیت در فضـای سایبـری کشور وجـود دارد و احتمـال نفوذ بالا به زیـر ساخت‌هـای کشور بـاعث شد تـا بـروز تهـدیداتی مـانند فلیم و اسـتاکس نت مهم‌تـرین رویدادهـای حـوزه افتـا در سال ۹۱ باشنـد زیـرا تاکنـون بـه مسئله امنیت سایبـری توجه زیـادی نشده بـود و راههـای نفـوذ بـرای سرقت اینترنتـی اطلاعـات موجود بـود تهدیـدات اخیـر مسئولین را نسبت به اهمیت حفظ امنیت این فضـا حساس کرد تا فعالیت‌هـای خود را در حـوزه امینت سایبـری بـا جدیت دنبـال کننـد.

مدیـرعـامل شرکت کارنما رایـانه می‌افـزاید: در حال حـاضر کشور مـا دشمنانی دارد که هدف آن‌هـا وارد آوردن خسارت است و در صورتـی که زمینه مناسب نفوذ برای وجود داشته باشد مسلمـا از آن به نفع خود استفـاده خواهنـد کرد پس لازم است راههـای نفـوذ افراد سودجو بـا دقت پوشش داده شود علاوه بر آن نبـاید توجه دشمنـان را به خود و فعالیت‌هـایمان جلب کنیم تا به دنبـال تخریب و ایجـاد اختلال در آن‌هـا باشنـد. در حال حـاضر اقداماتی در جهت حفظ امنیت صورت می‌گیـرد اما متاسفانه رونـد پیگیری آن‌هـا نسبت به سرعت پیشرفت ویروس‌هـا و بد افزارهـا بسیار کند است و لازم است جدی‌تـر دنبـال شوند.

وی با اشـاره به نقش مهم بخش خصوصی در افـزایش تـوان کشور در حفظ امنیت سایبری اظهار داشت: با توجه به اینکه تکنولوژی‌هـا از طریق بخش خصوصی وارد و تولیـد می‌شوند لازم است فعالیت‌هـای این بخش بیشتـر از سوی بخش دولتی دیده شده و مورد پذیرش قـرار گیرد. نگاه تجـاری که به حـوزه امنیت وجود دارد نیـز باعث کند شدن روند پیشرفت در این حوزه می‌شود جهت اصلاح این نگـاه لازم است بخش دولتی اقداماتی در جهت حمایت مالی از بخش خصوصی را در دستـور کار خود قرار دهـد تا این بخش فـارغ از مشکلات مـالی به افزایش دانش فنی، تحقیق، و تولید محصولات بومی بپردازد. زیـرا در درجـه اول لازم است دانش مورد نیاز تولید شود کـه این امر در گـرو صرف هزینه است و انجام تحقیقـات بودجه‌هـایی را می‌طلبد که تـامین آن در تـوان بخش خصوصی نیست.

دره شیـری همچنین افـزود: در شرایط فعلـی کشور تولیـد محصولات بـومی سرعت‌گیر تولیـدات است و ممکن است با کمی غفلت خسـارات زیادی وارد کنـد، بنابـراین لازم است همگـام با تلاش برای تولیـد محصولات بومی همچنـان مسئلـه مقـابلـه و دفـاع در مقـابل نفوذ بدافزارهـا و ویروس‌هـا مهم‌تـرین دغدغـه مسئولیـن امـر باشد تا با معطـوف شدن توجه به مسئله تولیـد محصولات بومـی از مسئلـه دفاع غـافل نشویم. همچنیـن از کارشنـاسانی استفاده کنیـم که با صداقت بیشتری فعالیت می‌کنند.

وی در خـاتمه خاطـر نشـان کـرد: هم اکنـون کشـور مـا دارای ارتش سایبری قدرتمنـدی است که نیاز به سلاح‌هـای قوی‌تـری دارد تا بتواند با تهدیدات مقابله کند، افزایش توان به منظور بـازدارندگی امری است که در شـرایط فعلـی باید بسیـار مورد توجه قـرار گیـرد تـا در درجـه اول با نفـوذ دشمنـان به مرزهـای سایبـری کشـور مقابلـه کنیم تـا از بروز خسـارات جلوگیـری شـود و به مـوازات آن از تلاش برای افـزایش دانش فنـی خود غـافل نشـویم.

دستورالعمل سایبری؛ دفاع سایبری

از سال ۱۳۸۹ با حمله ویروس استاکس نت به تاسیسات هسته‌ای کشور، کاربران، مسئولان و متخصصان حوزه امنیت بیش از گذشته بر وجود خطرات و آسیب‌پذیری‌های امنیتی تاکید و توجه کردند. در چنین شرایطی کشور ایران با توجه به شرایط ویژه و استراتژیکی که دارد وجود یک ارتش سایبری را برای دفاع از مرزهای مجازی کشور لازم و ضروری می‌داند. در این مورد با فرهمند آریا شکوه، مدیرعامل شرکت آرویـن رایان ارتباط گفت و گو کردیم که در ادامه می‌خوانید.

مهم‌ترین رویداد امنیتی حوزه افتا از دید شما در سال ۹۱ چیست؟

از مهم‌ترین رویدادهای سال ۹۱ می‌توان به حملات مخرب ویروس فلیم اشاره کرد. البته فلیم یک سلاح سایبری نبود بلکه فقط یک ابزار جاسوسی پیشرفته است. وقتی درباره جنگ‌افزار سایبری صحبت می‌کنیم منظور بدافزاری است که قادر است، خسارت فیزیکی ایجاد کند یا دست کم سیستم‌های کامپیوتری و نرم‌افزارها را تخریب کند. در حالیکه ویروس فلیم ابزاری پیشرفته برای جمع‌آوری اطلاعات از سیستم‌های کامپیوتری است. در چنین شرایطی به نظر می‌رسد فلیم یک ابزار جاسوسی سایبر و پیشرفته‌ترین ویروسی است که تاکنون وجود داشته است.

با توجه به اینکه کشور ما آماج حملات سایبری متعددی قرار گرفته، تحلیل شما از این رویدادها چیست و آینده را چطور ارزیابی می‌کنید؟

خوشبختانه در ایران نخبگان زیادی در زمینه امنیت فضای تبادل اطلاعات مشغول به فعالیت هستند. دفاع در مقابل حملات سایبری بسیار سخت‌تر از خود حمله است و تنها با دانش و تکنولوژی روز نمی‌توان جلوی آن را گرفت. در چنین شرایطی لازم است برای مقابله با حملات دانش کافی و شناخت لازم از محیط را به دست بیاوریم و کلیه عواملی که شکل و امنیت اینترنت را تغییر می‌دهد را شناسایی کنیم. در واقع رسیدن به یک محیط امن سایبری و فرهنگ جهانی امنیت مورد توجه کلیه کشورها است و می‌توان اینگونه پیش‌بینی کرد که هر چه حملات سایبری بیشتر باشند، متخصصان ایرانی نیز دانش بیشتری کسب خواهند کرد.

رویکرد بخش دولتی نسبت به حضور بخش خصوصی در حفظ امنیت سایبری کشور چیست؟

متاسفانه در کشور ما سازمان‌ها پس از وقوع مشکل و روبرو شدن با بحران، از کمک شرکت‌های امنیتی استفاده می‌کنند. اما متاسفانه نه برای تحلیل ویروس هزینه ای پرداخت می‌کنند و نه تمایلی به رسانه‌ای شدن موضوع دارند. چنین شرایطی در نهایت موجب ایجاد شکاف بین به خس دولتی و بخش خصوصی می‌شود. به اعتقاد من بخش دولتی باید قبل از هر چیز در تامین امنیت سازمان‌ها به بخش خصوصی اعتماد کند و پس از وقوع حمله اطلاعات را برای تحلیل در اختیار متخصصان قرار دهند.

عامل اساسی آسیب‌پذیری کشور در بحث امنیت را در چه زمینه ای می‌بینید؟ برای رفع آن چه راهکاری را پیشنهاد می‌کنید؟

همانطور که اشاره کردم متاسفانه دولتیان از رسانه‌ای کردن حملات ویروسی به سازمانشان واهمه دارند و همین امر سبب می‌شود تا ویروس‌ها با حداکثر آسیب‌رسانی به سازمان و بدون تحلیل و بررسی رها شوند.
در چنین شرایطی شرکت‌ها و دولت‌ها باید اطلاعات مربوط به حملات و جزئیات نفوذ به زیرساخت‌ها را افشا کنند تا آسیب‌پذیری‌های امنیتی موجود به راحتی شناسایی و برای مقابله با آن‌ها برنامه‌ریزی شود. ارتقای مدیریت ریسک، تضمین گزارش رویدادهای امنیتی مهم در محیط سایبری، دسترسی به اطلاعات مورد نیاز و... باید از جمله ضرورت‌های اجرایی در این حوزه باشد.

با توجه به اظهارات غرب در خصوص ارتش سایبری ایران، دیدگاه شما چیست؟ وجود ارتش سایبری تا چه اندازه در کنترل این گونه حملات کمک می‌کند؟ آیا قائل به وجود ارتش سایبری هستید یا افزایش توان به منظور بازدارندگی را توصیه‌می‌کنید؟

در طی سال‌های اخیر که کشور ما با افزایش حملات ویروسی روبه رو بوده است، نیاز به وجود یک راهبرد جدید سایبری نیز احساس شده است. راهبردی که از تعدادی دستورالعمل تشکیل شده، نوع سلاح مورد استفاده در صورت تصمیم به پاسخ نظامی و وقوع جنگ را معین می‌کند و در مورد شیوه همکاری با دولت‌های دوست و شرکت‌های خصوصی به منظور کاهش احتمال ورود خسارات و رفع تبعات آن‌ها تصمیم‌گیری کند.
اما در مجموع، این راهبرد می‌تواند دستورالعمل کلی برای زمان صلح، زمان وقوع درگیری وارتباط با کشورهای بی طرف را پیش‌بینی کند.
به هر ترتیب، راهبرد مورد بحث باید بر این منطق استوار شود که چنانچه کشور ایران از سوی هر کشور یا گروه تروریستی به صورت سایبری مورد هدف قرار گیرد، بتواند با هر اقدامی از جمله اقدامات نظامیِ فیزیکی نظیر انهدام سرورهای دولت یا گروه متخاصم، از خود دفاع کند و در مواردی نیز با اقدامات و حتی حمله پیشگیرانه، از وقوع حملات سایبری احتمالی در آینده جلوگیری کند.

جای خالی بخش خصوصی در شورای عالی فضای مجازی

با توجه به حساسیتی که فضای سایبر در دنیای امروز یافته است و ارتباط مستقیم آن با مسئله امنیت کشورها لزوم حراست از مرزها و حفظ قلمرو در این حوزه نیز از اهمیت بالایی برخوردار شده است. همچنین ورود ویروس‌ها و بد افزارها به زیر ساخت‌های حیاتی کشور می‌تواند خساراتی بیش ازجنگ‌های تن به تن بر کشور تحمیل کند. بنابراین لازم است با اعتماد به توان داخلی راهی مناسب برای مقابله با این دست تهدیدها طراحی شود.

بهناز آریا مدیر آموزش موسسه کهکشان نور و رئیس کمیسیون افتای سازمان نظام صنفی رایانه‌ای نیز معتقد است افزایش توان و آگاهی فارغ از موازی کاری‌ها راهیست که می‌تواند فضای سایبری کشور را در مقابل تهدید ویروس‌ها و بدافزارهای مخرب حفظ و حراست کند.

مدیر آموزش شرکت کهکشان در خصوص مهم‌ترین رویداد حوزه افتا در سال ۹۱ با اشاره به تهدیداتی مانند ویروس فلیم و تاثیر آن بر فضای سایبری کشور عنوان کرد: این ویروس‌ها علاوه بر خساراتی که به کشور وارد کردند باعث بروز رویکردی جدید در حوزه امنیت شدند. زیرا این ویروس‌ها که برای اولین بار با هدفی خاص جهت وارد آوردن خسارات مشخص طراحی شده بودند باعث بیداری امنیتی در سازمان‌ها و مجموعه‌های دولتی شدند تا نگاهی تخصصی به حوزه امنیت شکل گیرد و با مسئله امنیت سایبری به شیوه جدی‌تر برخورد شود.

بهناز آریا در ادامه می‌افزاید: در دنیای امروز نوع جنگ‌ها تغییر کرده و از جنگ تن به تن به جنگ‌های سایبری و الکترونیکی تبدیل شده است و حملات سایبری با موقعیتی که کشور در جامعه جهانی دارد عکس العمل طبیعی دشمن است و از این پس هم بیشتر اتفاق خواهد افتاد بنابراین لزوم وجود آمادگی برای مقابله با این تهدیدات بیشتر نمایان می‌شود.

وی همچنین در خصوص رویکرد بخش دولتی نسبت به بخش خصوصی عنوان کرد: در گذشته بخش دولتی و بخش خصوصی در حوزه امنیت تعامل خوبی با یکدیگر نداشتند اما با توجه به اتفاقات اخیر این رویکرد در حال تغییر است و بخش دولتی نیاز به همکاری با بخش خصوصی را بیشتر حس می‌کند با این وجود در حالی که تخصص و توان اجرایی در بخش خصوصی است هنوز هم در شورای عالی فضای مجازی کرسی برای بخش خصوصی وجود ندارد البته اخیرا اقداماتی در این خصوص صورت گرفته است اما شتاب بسیار کمی دارد.

رئیس کمیسیون افتای سازمان نظام صنفی رایانه‌ای اضافه کرد: در حال حاضر بخش دولتی تمایل زیادی به بومی‌سازی امنیت دارد که این امر تنها با مشارکت بخش خصوصی میسر خواهد شد البته تامین بودجه برای تولید سیستم عامل ملی و انجام تحقیقات در این زمینه از توان بخش خصوصی خارج و نیازمند حمایت مالی دولت است علاوه بر آن پس از تولید محصول فراگیر شدن آن نیز منوط به حمایت بخش دولتی است.

به اعتقاد وی در حال حاضر متخصصین خوبی در زمینه امنیت فضای سایبر در کشور وجود دارد اما مسئله اصلی که موجب آسیب‌پذیری می‌شود عدم هماهنگی و موازی کاری‌های متولیان این حوزه است که پیشرفت دانش و امکانات در این حوزه را کند کرده و توان پاسخ سریع به رویدادها را از ما سلب می‌کند. همچنین سطح آگاهی عمومی در خصوص امنیت سایبری بسیار پایین است. بنابراین لازم است با استفاده از تجربیات گذشته و بالا بردن سطح آگاهی عمومی ساز و کار مناسبی برای مقابله با تهدیدات ایجاد شود.

آریا معتقد است با توجه به میزان خساراتی که یک حمله سایبری به زیر ساخت‌های کشور وارد می‌کند باید تدابیر امنیتی مناسبی برای مقابله با آن‌ها اندیشیده شود. بنابراین لازم است مقابله‌ای با رویکرد تدافعی / تهاجمی طراحی شود تا در درجه اول توان خود را برای دفاع و بازگشت سریع به شرایط عادی افزایش دهیم و در صورت لزوم مقابله به مثل نیز داشته باشیم زیرا تهاجم بخشی غیر قابل اجتناب از جنگ و دفاع است.

رونق بخش خصوصی از طریق ساماندهی تولید و عرضه محصولات بومی

دیدگاه‌های سازمان فناوری اطلاعات در خصوص حوزه امنیت فضای تولید و تبادل اطلاعات

سازمان فناوری اطلاعات ایران به عنوان رگولاتور حوزه فاوا و زیرمجموعه‌های فعال آن از جمله مرکز ماهر به عنوان مرکز شناسایی تهدیدات سایبری، بدون شک نقش به سزایی در ساماندهی فعالیت‌های فناوری اطلاعات داشته‌اند. در خصوص دیدگاه‌های این سازمان راجع به امنیت فضای سایبر، گفتگوی مکتوبی با اسماعیل رادکانی، معاون گسترش فناوری اطلاعات انجام دادیم که در ادامه می‌خوانید.

مهم‌ترین رویداد امنیتی حوزه افتا از دید شما در سال ۹۱ چیست؟

مهم‌ترین رویداد امنیتی حوزه افتا از دیدگاه اکثر متخصصان، شناسایی بدافزار شعله آتش بوده که به فلیم نیز شناخته می‌شود. دلیل این امر آن است که شناسایی و پاکسازی این بدافزار اولین بار توسط متخصصین داخلی کشور (کارشناسان مرکز ماهر) شناسایی شد که نشانگر افزایش تجربه و توان آن‌ها بعد از مقابله با stuxnet است. فلیم از طریق حافظه‌های قابل حمل مانند فلش انتشار پیدا کرده و در سطح شبکه گسترش می‌یابد و مهم‌ترین هدف آن جاسوسی اطلاعات از سیستم‌های آلوده و ارسال اطلاعات ذخیره شده به خارج کشور می‌باشد. کارشناسان مرکز ماهر موفق به تولید ابزار شناسایی و پاکسازی بدافزار فلیم و اطلاع‌رسانی آن از طریق پرتال مرکز ماهر به آدرس www.Certcc.ir گردیده‌اند.

با توجه به اینکه کشور ما آماج حملات سایبری متعددی قرار گرفته، تحلیل شما از این رویدادها چیست و آینده را چطور ارزیابی می‌کنید؟

همانطور که مستحضر هستید، به دلیل نفوذ سیستم‌های مبتنی بر فناوری اطلاعات در کلیه شئون زندگی و همچنین شرایط حساس کشور، تهدیدات اینترنتی به منظور انجام حملات سایبری به فضای تبادل اطلاعات کشور افزایش قابل توجهی داشته است. تهدیدات و حملات سایبری به مراتب هزینه‌های کمتر و اثرات و پیامدهای حیاتی را به دنبال دارد و قطعاً در آینده حملات و تهدیدات پیچیده‌تر خواهند بود و نیاز به کسب آمادگی جهت پیشگیری و مقابله با آن‌ها در سطح کشور می‌باشد. در این راستا و با توجه به اقدامات انجام شده توسط کارشناسان مرکز ماهر، تهدیداتی با درجه اهمیت بالا با اهداف سرقت اطلاعات محرمانه، تخریب و دسترسی به اطلاعات سیستم قربانی شناسایی و راهکارهایی متناسب با تهدید به منظور مقابله با آن‌ها ارائه گردیده است.

رویکرد بخش دولتی نسبت به حضور بخش خصوصی در حفظ امنیت سایبری کشور چیست؟

رویکرد بخش دولتی استفاده حداکثری از بخش خصوصی در حفظ امنیت سایبری کشور است. در همین راستا قراردادها و تفاهم نامه‌های تخصصی با مراکز معتبر علمی تخصصی به منظور فعال‌سازی بخش خصوصی در حال انجام می‌باشد.

از آن جمله می‌توان به مواردی همچون انعقاد تفاهم نامه و قراردادهای تخصصی با مراکز دانشگاهی و صنعتی کشور. حمایت از توسعه توانمندی‌ها و ظرفیت‌های بومی داخلی در حوزه فناوری اطلاعات، رتبه بندی و به کار گیری شرکت‌های فعال در حوزه امنیت و ارزیابی محصولات امنیتی فتا اشاره نمود.

نقش دولت در توانمندسازی بخش خصوصی در تولید محصولات بومی چیست؟

آزمایشگاه‌هایی به منظور ارزیابی کیفی محصولات سخت‌افزاری و نرم‌افزاری تولید شده توسط شرکت‌های خصوصی در حوزه امنیت تشکیل شده که به شرکت‌هایی که محصولات آن‌ها بتوانند تست‌های کیفی استاندارد مربوطه را بگذرانند، گواهینامه تایید محصول داده می‌شود.

با توجه به اینکه بخش دولتی در حوزه امنیت موظف به خرید تجهیزات بومی می‌باشد یقیناً ساماندهی تولید و عرضه محصولات بومی و ایجاد بازار برای آن‌ها باعث رونق کسب و کار بخش خصوصی می‌گردد.

عامل اساسی آسیب‌پذیری کشور در بحث امنیت را در چه زمینه‌ای می‌بینید؟ و برای رفع آن‌ها چه راهکاری را پیشنهاد می‌کنید؟

با توجه به تجربیات کسب شده در خصوص فعالیت و همکاری با سازمان‌ها و دستگاه‌های اجرایی کشور در حوزه افتا مشکلاتی از قبیل عدم آگاهی و دانش نا کافی کارشناسان و مدیران درگیر در این حوزه و عدم توجه و تاکید مناسب بر ایمن‌سازی سیستم‌های اطلاعاتی سازمان‌ها دارای اهمیت می‌باشد.

به منظور ارتقا سطح ایمنی سیستم‌ها و شبکه‌های سازمانی کشور می‌توان به راهکارهایی از جمله توسعه نظام متد پیشگیری و مقابله با حوادث رایانه‌ای در سطح کشور، استقرار نظام ملی مدیریت امنیت اطلاعات با هدف اجرای سیستم مدیریت امنیت اطلاعات در کلیه دستگاه‌ها، و برگزاری دوره‌های آموزشی تخصصی در حوزه امنیت فناوری اطلاعات می‌توان اشاره نمود.

با توجه به اظهارات غرب در خصوص ارتش سایبری ایران، دیدگاه شما چیست؟ وجود ارتش سایبری تا چه اندازه در کنترل اینگونه حملات کمک می‌کند؟ آیا قائل به وجود ارتش سایبری هستید یا افزایش توان به منظور بازدارندگی را توصیه می‌کنید؟

قطعاً اگر تهدیدی تمامیت ارضی و موجودیت نظام جمهوری اسلامی ایران را تهدید کند، همه ما موظفیم از کلیه توان و امکانات خود در جهت پاسداری از کشور و نظام استفاده نماییم و توان خود را در زمینه بازدارندگی افزایش دهیم.

آینده حملات سایبری به زیر ساخت‌های حیاتی کشور را چگونه ارزیابی می‌کنید؟ در سطح کلان کشور چه راهبردهایی را در این زمینه پیشنهاد می‌نمایید؟

انجام حملات هدفمند با هدف تخریب، سرقت اطلاعات و آسیب رسانی به زیر ساخت‌های حیاتی و سیستم‌های اطلاعاتی سازمان‌ها یکی از پر تکرارترین تهدیدات رایانه‌ای در کشور می‌باشد. کشور ما نیز از این قاعده مستثنی نبوده و با توجهبه شرایط حساس کشور مورد هجوم حملات و تهدیدات سایبری با اهداف کسب اطلاعات سازمانی، مالی، صنعتی و سیاسی است. بر طبق گزارش سازمان بین المللی اطلاعات (IDC) هزینه‌های جهانی ایجاد امنیت بیش از ۷۰ میلیارد دلار در سال ۲۰۰۳ بوده که این هزینه‌ها در سال ۲۰۰۸ به ۱۱۶ میلیارد دلار رسیده است.

با توجه به بررسی‌های صورت گرفته، دولت‌ها و کشورها در سطح دنیا اقدام به انعقاد تفاهم نامه‌ها و اختصاص سرمایه گذاری‌های مناسب در زمینه مدیریت کلان برنامه‌ها و طرح‌های امنیت این فضا و امن سازی زیر ساخت‌های حیاتی نموده‌اند.

لذا به منظور ایمن‌سازی زیرساخت‌های اطلاعاتی کشور می‌بایست راهبردهایی از جمله تقویت و پیاده سازی زیر ساخت‌های پایش و مانیتورینگ فضای تولید و تبادل اطلاعات کشور، ارتقا سطح دانش تخصصی کارشناسان و مدیران درگیر در این حوزه مورد نظر می‌باشد.

ابزارهای بومی یک راه‌حل مطمئن برای حفظ امنیت

بحث بر سر استفاده از ابزارهای امنیتی بومی و یا ابزارهای خارجی بحث دیروز و امروز نیست. از زمانیکه اینترنت به عنوان جزئی از زندگی تکنولوژیک انسان‌ها شناخته شد، توجه کاربران به امنیت در این فضا نیز جلب شد. از همان زمان عده‌ای بر استفاده از ابزارهای امنیتی بومی برای حفظ امنیت فضای سایبر تاکید کردند. آنی خاچیکیان نیز از همان دسته افرادی است که معتقد است در کنار رعایت استانداردهای بین المللی باید یک استراتژی امنیتی داخلی هم برای کشور داشته باشیم. در ادامه گفت و گوی افتانا با مدیر عامل شرکت پویه را بخوانید.

با توجه به این که کشور ما آماج حملات سایبری متعددی قرار گرفته، تحلیل شما از این رویدادها چیست و آینده را چطور ارزیابی می‌کنید؟

جهان پیرامون ما در حال گذار از وضعیت جهانی هویت‌های فیزیکی به جهانی هویت‌های مجازی است. بطوریکه می‌توان گفت هم اکنون به ازای هر هویت فیزیکی حداقل یک هویت مجازی در جهان مجازی نیز وجود دارد. از این رو جنگ‌ها، مسابقه‌ها و کشمکش‌هایی که علیه یک هویت فیزیکی می‌تواند وجود داشته باشد در جهان مجازی نیز با ابزارهای خاص خود نیز وجود دارد.

با پیچیده‌شدن ابزارهای تکنولوژی، فضای مجازی و همچنین افزایش ارتباطات هویت‌های مجازی با یکدیگر و توجه به این هویت‌ها، سوءاستفاده از این فضا نیز جذابیت بیشتری پیدا کرده است و از آنجائیکه امکان عقب نشینی و بستن این فضا وجود ندارد، پس بهترین راهکار بالا بردن دانش در این عرصه و همگام شدن با تکنولوژی روز است.

در کشور ما اگرچه جریان افزایش دانش وجود دارد اما لازم است هویت‌های مجازی موجود در این فضا سازمان دهی شده و ساختار سازمانی آن‌ها همیشه در حال رشد، توسعه و بازبینی باشد. همچنین استانداردسازی، ایجاد ارتباطات محلی برای تعاملات بین سازمانی این هویت‌های چندگانه نیز نیازمند وقت و کار بیشتر است. در چنین شرایطی می‌توان ادعا کرد در آینده به مراتب کمتر از آنچه امروز در معرض خطرات فضای سایبر قرار داریم، قرار خواهیم داشت.

رویکرد بخش دولتی نسبت به حضور بخش خصوصی در حفظ امنیت سایبری کشور چیست؟

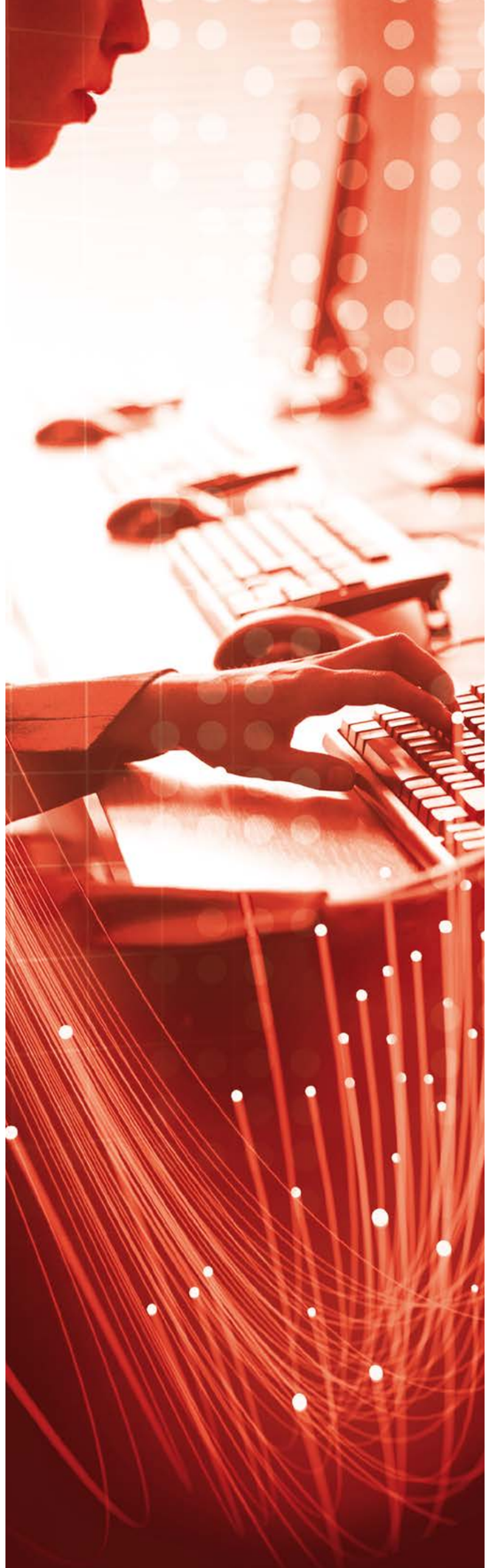
نیاز بخش دولتی به بخش خصوصی در استانداردسازی، توسعه و تحقیق همگام با آموزش مشهود و مشارکت بخش خصوصی در این زمینه اجتناب‌ناپذیر است. چرا که این دو بخش هر کدام پتانسیل‌های مخصوص به خود را دارند و باید پذیرفت دولت به تنهایی و بدون مشارکت بخش خصوصی چندان کارآمد نخواهد بود. پس اگر بخش دولتی به دنبال دستیابی به بیشترین کارایی در حفظ امنیت سایبری است چاره‌ای جز استفاده از پتانسیل‌های بخش خصوصی نخواهد داشت.

نقش دولت را در توانمندسازی بخش خصوصی در حفظ امنیت سایبری کشور تا چه حد ارزیابی می‌کنید؟

قطعاً دولت می‌تواند در ایجاد فضای توسعه و تولید و همچنین حمایت از بخش خصوصی و در کنار همه این‌ها و از همه مهم‌تر ایجاد ثبات در عرصه‌های اقتصادی از بخش خصوصی حمایت کند. همانطور که قبلاً هم اشاره کردم، بخش دولتی و بخش خصوصی بدون کمک به یکدیگر کارایی به مراتب کمتری در حفظ امنیت سایبری کشور و استفاده از پتانسیل‌ها خواهند داشت.

عامل اساسی آسیب‌پذیری کشور در بحث امنیت را در چه زمینه‌ای می‌بینید؟ و برای رفع آن چه راهکاری را پیشنهاد می‌کنید؟

اگر چه کلیه کشورها و از جمله ایران باید با استانداردهای بین‌المللی هماهنگ باشند و این مسئله امری اجتناب‌ناپذیر است اما در کنار آن باید به این موضوع نیز توجه کرد که وابستگی بیش از حد به اجزای امنیتی خارجی می‌تواند کشور را با مخاطرات امنیتی روبرو کند.
در حقیقت توانایی بومی در عرصه امنیت اطلاعات و خدمات، ضامن امنیت و توسعه آتی آن و همگام بودن با دنیا خواهد بود. در حقیقت داشتن توانایی بومی در کنار حفظ کشور در مقابل آسیب‌پذیری‌های امنیتی شرایط صادرات محصولات و همچنین ارائه خدمات به سایر کشورها را فراهم خواهد کرد.



حمله راه حل نیست؛ آموزش دهید

اگرچه چند سالی می‌شود که امنیت اطلاعات در نظر کاربران مهم‌تر و اساسی‌تر از گذشته جلوه کرده است اما شاید بتوان گفت بالا و پایین‌های سال ۹۱ در این حوزه بیشتر از هر سالی نمود کرده است.
در حالی که سال ۹۱ به پایان خود نزدیک می‌شود، فرصت مناسبی است تا پای صحبت‌های فعالان این حوزه بنشینیم و به بررسی اوضاع امنیت اطلاعات در سالی که گذشت بپردازیم. در ادامه گفت‌وگوی افتانا با حمیدرضا سعدی مدیر عامل شرکت مهران رایانه می‌خوانید.

مهم‌ترین رویداد امنیتی حوزه افتا در سال ۹۱ از دیدگاه شما چیست؟

متاسفانه کشور ما در سال ۹۱ با حملات گسترده سایبری روبرو بود که بخشی از آن‌ها توسط کارشناسان شناسایی و کشف شد و از کنار تعدادی از آن‌ها نیز بی توجه رد شدند. اما از میان همه آن‌ها آنچه به اعتقاد من توانست به کشور ضربه وارد کند، حمله ویروس شعله (Flame) به سیستم‌های وزارت نفت و زیر مجموعه‌های تابعه آن بود. چرا که متاسفانه باعث قطعی دو ماهه اینترنت در این وزارتخانه و ایجاد اختلال در امور جاری شد و این اتفاق قطعاً هزینه‌های زیادی را به کشور تحمیل کرد.

با توجه اینکه کشور ایران طی سال‌های اخیر آماج حملات سایبری شده است. لطفاً تحلیل خود را از علت بوجود آمدن چنین شرایطی بفرمائید و آینده را چطور ارزیابی می‌کنید؟

مهم‌ترین وظیفه کشور در مقابل حملات سایبری دفاع است چرا که با شرایط فعلی به نظر می‌رسد که در آینده نیز اینگونه حملات افزایش خواهد داشت. به نظرم وجود چنین شرایطی در کشور به دلیل استفاده از ابزارهای امنیتی خارجی است. اگرچه مصوبه استفاده از نرم افزارهای داخلی در کشور ابلاغ شده است اما با وجود کاربرانی که از نرم افزارهای امنیتی قفل شکسته رایگان استفاده می‌کنند و همچنین سازمان‌های بزرگی که اعتقادی به استفاده از محصولات داخلی ندارند، نمی‌توان انتظار دفاع در مقابله با این حملات را داشت. این نکته که نرم افزارهای امنیتی خارجی قابلیت‌ها و همچنین امکانات بهتری نسبت به نرم افزارهای تولید داخل دارند قابل قبول است اما استفاده از آن‌ها توجیه امنیتی ندارد. این موضوع مانند این است که بگوییم سربازان امریکایی از سربازان ایرانی بهتر هستند و لب مرز کشور از آن‌ها استفاده کنیم آیا خط مشی آن‌ها حفاظت از ما است؟ این درحالیست که متاسفانه در ۹۵ درصد از سازمان‌های دولتی در خط مقدم امنیتشان از محصولات خارجی استفاده می‌کنند. با وجود چنین تفکری چطور می‌توان انتظار داشت در مقابل حملات سایبری مقاومت کنیم؟

به نظر شما رویکرد بخش دولتی نسبت به حضور بخش خصوصی در حفظ امنیت سایبری کشور چیست؟

متاسفانه دولتی‌ها با بخش خصوصی غریبه هستند. تا زمانیکه از محصول خارجی استفاده می‌کنند و همه چیز مرتب است، سراغی از تولیدکننده داخلی نمی‌گیرند اما به محض اینکه با مشکلی مواجه شوند انتظار دارند محصولی به مراتب بهتر از محصولات خارجی و با قیمت پائین‌تر به آن‌ها ارائه کنیم.

با این توضیح نقش دولت را در توانمندسازی بخش خصوصی در تولید محصولات بومی کمرنگ می‌دانید؟

به اعتقاد من اگر در کشور قانون کپی رایت رعایت می‌شد و کاربران به صورت رایگان به نرم افزارهای مختلف دسترسی نداشتند، شرایط برای پرورش نبوغ بخش خصوصی و تولید نرم افزارهای بومی نیز فراهم می‌شد. اما متاسفانه به دلیل عدم حمایت دولت و عدم وجود چنین قانونی کاربران به راحتی و البته رایگان به انواع نرم افزارها دسترسی دارند و حاضر نیستند برای نمونه داخلی آن پول بدهند. در چنین شرایطی و بدون وجود بازار، تولید مقرون به صرفه نخواهد بود. در بحث امنیت که بسیار مهم و حیاتی است نیز با چنین شرایطی روبرو هستیم متاسفانه دولتی‌ها اقدامی برای بهبود شرایط بازار نمی‌کنند و بازار خودش را با شرایط تطابق می‌دهد. مثلاً در زمینه نرم افزارهای حسابداری که امکان استفاده از نرم‌افزارهای خارجی وجود ندارد، شرکت‌های خصوصی به خوبی وارد عمل شده و نرم افزارهای خوبی هم ارائه کرده‌اند اما در سایر زمینه‌ها که خارجی‌ها بازار را قبضه کرده‌اند، دولت نیز اقدامی برای برون رفت از این شرایط انجام نمی‌دهد.

پس می‌توان اینطور نتیجه گرفت که به اعتقاد شما راهکار برون رفت از آسیب پذیری‌های امنیتی اجبار دولت‌ها به استفاده از نرم‌افزارهای داخلی است؟

البته اجبار بدون زمینه‌سازی قبلی بی‌نتیجه خواهد بود. نمی‌توان از دولت انتظار داشت در این زمینه سازمان‌ها را مجبور به استفاده کند اما زیرساخت و سرمایه‌گذاری در این حوزه وجود نداشته باشد. به عنوان مثال نمی‌توان انتظار داشت کاربران گوشی‌های داخلی دستشان بگیرند اما تولید کننده گوشی داخلی نداشته باشیم. قبل از هر چیز دولت باید شرایط انگیزشی را برای سرمایه‌گذاری در این حوزه فراهم کند اگر این اتفاق نیفتد اجبار به ضرر تولید کننده داخلی تمام خواهد شد.

باتوجه به اظهارات اخیر غرب در خصوص ارتش سایبری ایران لطفاً دیدگاه خود را در این خصوص بفرمائید. وجود چنین ارتشی تا چه اندازه در کنترل حملات موفق خواهد بود؟

روزانه بیش از ۱۵۰ هزار فایل آلوده در کشور شناسایی می‌شود، ارتش سایبری با چه تعداد نیرو قرار است در مقابل این حملات بایستد؟ دفاع و حمله لازم و ملزوم یکدیگر هستند آیا دولت قصد دارد تنها از طریق حمله در مقابل سایر حملات دفاع کند. این درحالیست که می‌توان گفت ۸۰ درصد حملاتی که به کشور وارد می‌شود، از روی سهل انگاری کاربران است. پس اگر به کاربران شیوه درست حضور در فضای سایبری آموزش داده شود از هر دفاع و حمله ای اثربخش‌تر خواهد بود.

کشور نیازمند ایجاد بازار شفاف و رقابتی در تولید محصولات بومی است

در شرایط فعلی که فضای مجازی به میدان جنگ میان کشورها تبدیل شده و حفظ امنیت آن یکی از مهم‌ترین دغدغه‌های کشورهای مختلف است؛ داشتن آگاهی کامل از جنبه‌های مختلف امنیت این فضا و دیدگاهی روشن نسبت به امکانات و دانش فنی متخصصان کشور، می‌تواند امکان دفاع از مرزهای مجازی و مقابله با تهدیدها را فراهم کند. در ادامه گفتگوی افتانا با مهندس فریدالدین مهروانی بهبهانی مدیرعامل شرکت ایده فروزان امن (اینفوامن) در این خصوص را می‌خوانید.

مهم‌ترین رویداد امنیتی حوزه افتا از دید شما در سال ۹۱ چیست؟

به عقیده من مهم‌ترین رویداد سال جاری آشکار شدن حمله هدفمند به شبکه‌ها و سیستم‌های اطلاعاتی کشور توسط بدافزارهای Flame و SkyWiper بود که مشخصاً از مدت‌ها پیش به صورت خاموش در حال نفوذ به سیستم‌ها بوده‌اند.

با توجه به اینکه کشور ما آماج حملات سایبری متعددی قرار گرفته، تحلیل شما از این رویدادها چیست و آینده را چطور ارزیابی می‌کنید؟

فضای سایبری، روز به روز بیشتر به محیط چالش قدرت‌ها تبدیل می‌شود و تخاصمات به صورت بسیار سریعی از فضای واقعی به فضای سایبری منتقل می‌گردد. با این نگاه انتظار می‌رود این روند ضمن گسترش، با بلوغ بیشتری نیز همراه شده و نوع عملیات و رویکرد به حملات، پیچیده‌تر و چند وجهی‌تر گردد، به گونه‌ای که شاید بتوان آنرا جنگ سرد قرن ۲۱ نامید.

رویکرد بخش دولتی نسبت به حضور بخش خصوصی در حفظ امنیت سایبری کشور چیست؟

این رویکرد البته در صورتی که بتوان آن را به عنوان رویکرد شناسایی کرد، در واقع نگاه و برخورد بخش دولتی از هدفمندی و انسجام لازم برای یک «رویکرد» محروم است، عمدتاً بر مبنای نگاه حداقلی به بخش خصوصی و در بهترین شرایط خواهان سپردن امور «غیر حیاتی» امنیت به بخش خصوصی است. در صورتی که دیدی جامع و صحیح از اوضاع و شرایط نزد تصمیم گیرندگان موجود باشد، این نگاه نیازمند بازنگری اساسی است؛ چرا که در فضای جدید تهدیدات سایبری، یک کشور نیاز به تقویت جامع و کامل محیط سایبری و کاربران سایبری (حتی در بخش‌های غیردولتی) دارد. در عین حال به نظر می‌رسد از زاویه تعریف و نگاه به امنیت نیز شکافی بین بخش دولتی و بخش خصوصی مشهود است، به گونه‌ای که ادبیات تعامل این دو بخش در فضای امنیت متفاوت و ناهمگون شده است.

نقش دولت در توانمندسازی بخش خصوصی در تولید محصولات بومی چیست؟

بهترین نقشی که دولت در این خصوص می‌تواند ایفا نماید ایجاد بازار تقاضای «شفاف» و «رقابتی» در حوزه محصولات و فناوری‌های امنیتی بومی است، عملی که دولت‌های پیشرو در این عرصه، از دهه‌ها قبل آغاز نموده‌اند. به این ترتیب علاوه بر تولید محصولات و فناوری‌های بومی که می‌تواند مورد استفاده بخش دولتی و خصوصی قرارگیرد، نیروی متخصص مورد نیاز کشور جهت فعالیت در بخش‌های حساس‌تر و نیز پروژه‌های امنیتی- نظامی در دامن بخش خصوصی رشد و نمو کرده و به صورت واقعی توانمندی‌های لازم را کسب می‌نمایند.

عامل اساسی آسیب‌پذیری کشور در بحث امنیت را در چه زمینه‌ای می‌بینید؟ و برای رفع آن چه راهکاری را پیشنهاد می‌کنید؟

مهم‌ترین عامل آسیب‌پذیری کشور، نگاه ناکارآمد به امنیت از دو جنبه است:

الف) نگاهی که با سهل‌گیری بیش از حد تبعات بروز رخدادهای امنیتی را دست کم می‌گیرد و مسائلی مانند حمله‌های سایبری فلج کننده را در حد افسانه می‌پندارد.

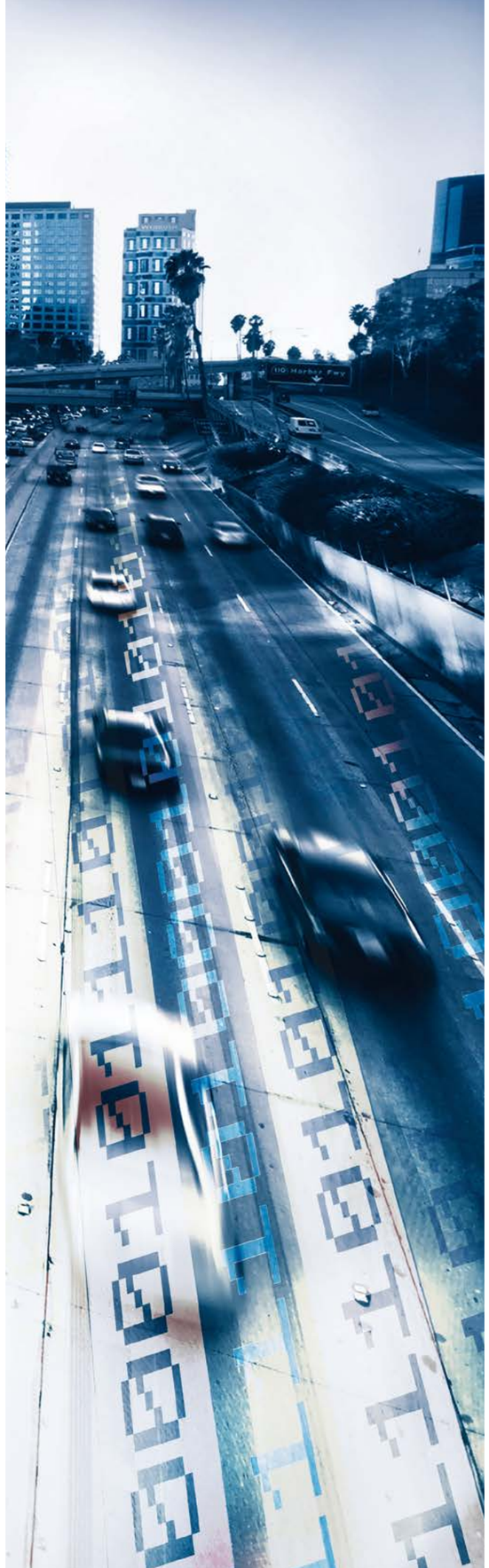
ب) نگاهی که دغدغه امنیت را به صورت جدی دارد، لیکن به دلیل ضعف در بعد فناوری یا درک ناکامل فضا و الزامات مدرن، ناتوان از برقراری امنیت است و اقداماتی نسنجیده را تجویز می‌نماید که یا غیرعملی بوده و یا بی اثر می‌باشد.

جهت رفع این معضل بنیادی می‌باید نخبگان با هر دو نگاه (با پیش زمینه امنیتی- حاکمیتی و تخصصی- فنی) گرد آمده و راهکارهایی مناسب و جامعی تدوین نماید که به عنوان تاکتیک‌های امنیت سایبری در سطح ملی قابل استفاده باشد.

با توجه به اظهارات غرب در خصوص ارتش سایبری ایران، دیدگاه شما چیست؟ وجود ارتش سایبری تا چه اندازه در کنترل این گونه حملات کمک می‌کند؟ آیا قائل به وجود ارتش سایبری هستید یا افزایش توان به منظور بازدارندگی را توصیه‌می‌کنید؟

وجود ارتش سایبری (با نام و ساختار متفاوت) در هر کشوری به عنوان یک جنبه دفاعی و نظامی مدرن امری طبیعی و قابل انتظار است. البته عموماً فعالیت‌های این نهادها یا جنبه تهاجمی دارد و یا مقابله به مثل؛ لذا به عنوان نیرویی بازدارنده یا دفاعی، نمی‌توان نقشی شاخص برای آن متصور بود. بنابراین ضمن عدم نفی جنبه‌های استراتژیک وجود چنین نهادهایی در حوزه سایبری، ایجاد جنبه‌های بازدارنگی و دفاعی/ پدافندی نیاز به رویکرد جامع‌تری در رفع آسیب‌پذیری‌ها و مدیریت تهدیدها در سطح ملی (نه تنها دولتی) دارد.

تجارت امن



تولید محصولات بومی، مکمل نیازملی

نوع نگاه دولت به توانمندی‌های بخش خصوصی همواره از مسائلی بوده که انتقادهایی را در پی داشته است. از سویی دیگر بخش خصوصی سعی کرده است با ارائه توانمندی‌ها، قابلیت‌ها و امکانات خود در نوع نگاه و نگرش بخش دولتی تغییر ایجاد کند.

رضا اخلاقی، مدیرعامل شرکت دمسان رایانه ضمن گله‌مندی از بخش دولتی و نگاه حذفی آنان به محصولات امنیتی، تولید محصولات مکمل در داخل را از نقش‌های مهم دولت می‌داند.

وی در گفتگو با افتانا، کشف ویروس مخرب فلیم را از مهم‌ترین رویدادهای امنیتی در سال ۹۱ دانست و با وجود دغدغه‌هایی که در آن زمان به وجود آورده بود، بازتابی را که در بیداری مدیران و کارشناسان شبکه داشته را از جنبه‌های مثبت آن عنوان کرد.

با توجه به اینکه کشور ما آماج حملات سایبری متعددی قرار گرفته، ایشان با بیان اینکه جنگ مورد نظر سال‌هاست که آغاز گشته و روز به روز بر شدت و وسعت آن افزوده می‌شود، گفت: در این شرایط قطعاً هر کسی که آماده دفاع نباشد محکوم به نابودی است.

رضا اخلاقی در رابطه با رویکرد بخش دولتی نسبت به حضور بخش خصوصی در حفظ امنیت سایبری کشور، نگاه بخش دولتی را تاکنون به محصولات امنیتی نگاهی حذفی دانست و تصریح کرد: دولت به جای بررسی و پیداکردن نقاط ضعف و سعی در پوشش آن با روش‌های مکمل همیشه ترجیح داده است که صورت مساله را پاک کند که این روش جز ایجاد ضرر مضاعف برای دولت نتیجه دیگری نخواهد داشت.

مدیرعامل شرکت دمسان رایانه، در رابطه با نقش دولت در توانمندسازی بخش خصوصی در تولید محصولات بومی، توضیح داد: در تولید داخلی ما همیشه ضعیف بوده‌ایم زیرا به جای حرکت در امتداد تکنولوژی همیشه سعی داشته‌ایم که چرخ را مجدداً اختراع کنیم، و به دلیل فاصله زیاد ما با مخترعین اصلی آن، کیفیت و کمیت در تولیدات‌مان زیر سوال بوده است. به جای اینگونه اعمال، راهبرد دولت باید این باشد که به تولید محصولات مکمل بپردازد، تا در این راستا نقاط ضعف (یا موارد مورد حساسیت حاکمیت) را در محصولات خارجی موجود، نسبت به نیاز داخلی پوشش دهد. با این روش علاوه بر رسیدن به هدف در زمان قابل قبول، نگرانی‌های امنیتی نیز پوشش داده می‌شود و می‌توان سیستمی جهت واکنش سریع به رخداد متمرکز بوجود آورد که بهبود قابل توجهی از نظر امنیت شبکه در کشور را به همراه خواهد داشت.

وی اصلی‌ترین مشکل و عامل اساسی آسیب‌پذیری در بحث امنیت در داخل کشور را فقدان دانش در مجاری تصمیم‌گیری و نقاط اجرایی کشور دانست و یادآور شد این عامل باعث شده که حتی از امکانات کم موجود هم نتوانیم به درستی و به موقع در زمان نیاز استفاده نماییم. اخلاقی تاکید کرد: افزایش دانش جزو مهم‌ترین نیازهای کشور در زمینه امنیت سایبری می‌باشد.

با توجه به اظهاراتی که غرب در خصوص ارتش سایبری ایران داشته است، ایشان با توجه به ضرورت ارتش در جنگ متذکر شد: همانطور که در توضیحات قبل هم گفته شد، این یک جنگ است و در هر جنگی نیاز به ارتش ضروری است. البته بنده به مقوله ارتش سایبری صرفا به شکل تهاجمی آن نگاه می‌کنم و بحث پدافند را جدا از ارتش سایبری می‌دانم.

در انتها مدیرعامل شرکت دمسان رایانه در رابطه با کنترل اینگونه حملات گفت: هر چه ارتش در یک کشور قوی‌تر باشد دیگران نیز متقابلاً در حمله به آن ملاحظه بیشتری می‌کنند.

تجارت امن

فرهنگ‌سازی خط مقدم امنیت

اگرچه به اعتقاد مدیر عامل شرکت رایان سامانه آرکا، هر روز که می‌گذرد بر تعداد ویروس‌ها و بدافزارهایی که با نیت حمله سایبری به کشور وارد می‌شوند، افزوده می‌شود اما می‌توان با آموزش تک تک کاربران به عنوان دروازه‌های ورودی بدافزارها با حد زیادی از هجوم این حملات کاست. در ادامه گفتگوی افتانا با آیدین مهدی‌پور مدیرعامل شرکت رایان سامانه آرکا را بخوانید.

مهم‌ترین رویداد امنیتی حوزه افتا از دید شما در سال ۹۱ چیست؟

به طور قطع در حوزه تهدیدات سایبری سال پر تهدیدی را پشت سر گذاشتیم. اما به اعتقاد من مهم‌ترین تهدیدی که در این سال با آن روبرو بودیم، بدافزار شعله آتش (Flame) بود. البته این اتفاق جنبه مثبتی هم داشت و توانست موجی نو از توجه به امنیت را در جامعه ایجاد کند. همچنین تصمیمات عجیب و مقطعی اتخاذ شده در این سال را نیز می‌توان جزء رویدادهای مهم سال ۹۱ دانست. از این نوع دستورات عجیب می‌توان به دستور وزیر پیشین ICT مبنی بر ممنوعیت ورود محصولات امنیتی اشاره کرد. اگر هم بخواهیم به بررسی مهم‌ترین رویداد سال ۹۱ از منظر صنفی نگاه کنیم می‌توان تشکیل کارگروه ساماندهی ضدبدافزارهای خارجی را نام برد که امیدوارم این کارگروه به بازار نابسامان ضدبدافزارها کمک کند.

با توجه به اینکه کشور ما آماج حملات سایبری متعددی قرار گرفته، تحلیل شما از این رویدادها چیست و آینده را چطور ارزیابی می‌کنید؟

وقوع حملات سایبری به کشور اتفاق تازه‌ای نیست. با توجه به افزایش تعداد کاربران اینترنت و همچنین هوشمند شدن آن‌ها نیز این حملات افزایش چشمگیری داشته است. اما از یک سو چندین برابر شدن حملات و از سوی دیگر شناسایی بدافزارهایی همچون شعله که با هدف خاص و ویژه جاسوسی طراحی شده است، نشان دهنده شروع جنگی از سوی دشمنان است. با بررسی تهدیداتی که طی سال‌های اخیر به کشور وارد شده است، می‌توان این طور نتیجه گرفت که در آینده نه تنها از حجم این تهدیدات کاسته نخواهد شد، بلکه افزایش چشمگیری هم خواهد یافت. در چنین شرایطی توجه به حفظ امنیت و همچنین استفاده از ابزارهای امنیتی اهمیت ویژه‌ای پیدا می‌کند.

رویکرد بخش دولتی نسبت به حضور بخش خصوصی در حفظ امنیت سایبری کشور چیست؟

پیش از اینکه پاسخ سئوال شما را بدهم، باید نیم نگاهی داشته باشم به شرکت‌های خصوصی و توانمندی آن‌ها و پاسخ به این سئوال که بخش خصوصی در حفظ امنیت سایبری چه نقشی را می‌تواند ایفا کند؟

همزمان با رشد بازار فناوری اطلاعات در ایران، می‌توان گفت شرکت‌های فعال در حوزه افتا به بلوغ نسبی رسیده‌اند. به این معنی که بسیاری از محصولاتی که امکان تولید آن در داخل کشور وجود دارد، بومی‌سازی شده و توسط شرکت‌های داخلی تولید شده‌اند. اما در بین آن دسته از محصولات که امکان تولید آن در داخل وجود ندارد محصولات مناسب و با کیفیت نیز انتخاب و بهترین محصولات توسط نمایندگان معتبر در داخل کشور ارائه می‌شود. خوشبختانه نمایندگان فروش محصولات امنیتی خارجی، به فروش محصول به تنهایی بسنده نکرده و پشتیبانی مناسبی هم ارائه می‌دهند. علاوه بر ارائه محصول، در بخش خدمات هم تعداد زیادی از مشاوران امنیت فناوری اطلاعات ایران که دارای بالاترین درجات فنی و مهندسی هستند کار را در دست گرفته‌اند و از عهده مهندسی امنیت اطلاعات برمی آیند.

اما متاسفانه می‌بینیم با وجود چنین توانمندی‌های مناسبی که در بین شرکت‌های خصوصی وجود دارد، همچنان بخشی از مدیران دولتی به شرکت‌های خصوصی اعتماد ندارند و در زمان تصمیم‌گیری‌های کلان برای کشور، توجهی به نظرات بخش خصوصی نکرده و قانون‌گذاری می‌کنند. در نهایت نیز شرکت‌ها ملزم به رعایت قانونی هستند که هیچ نقشی در تدوین آن نداشته‌اند.

با این شرایط نقش دولت را در توانمندسازی بخش خصوصی و تولید محصولات بومی تا چه حد اساسی و ضروری می‌بینید؟

در سال‌های گذشته شاهد رشد تخصص متخصصان ایرانی در حوزه فناوری اطلاعات بودیم. به طوریکه شرکت رایان سامانه آرکا در سال ۹۱ موفق به رونمایی از چندین محصول داخلی و بومی شد. به عنوان مدیر یک شرکت دانش بنیان که چنین تولیداتی را در سال ۹۱ ارائه کرده است، معتقدم بزرگ‌ترین مشکل ما جلب اعتماد مدیران دولتی است. مساله‌ای که قبلاً هم به آن اشاره کردم.

به اعتقاد من برای رفع این مشکل و استفاده از پتانسیل‌های قوی موجود در بخش خصوصی، دولتمردان باید با ایجاد آزمایشگاه‌های بزرگ برای بررسی تهدیدات و فراهم کردن زیرساخت‌های آن، راه توانمندسازی بخش خصوصی را در تولید محصوات ملی و بومی هموار کنند. در کنار این اقدام، حمایت از تولید داخل با تشویق و نه اجبار سازمان‌ها به خرید محصولات داخلی نیز یکی دیگر از راهکارهایی است که به توانمندی بخش خصوصی کمک می‌کند.

اما در نهایت مسئله مهم فروش محصولات در بازارهای جهانی است متاسفانه بعد از آنکه همه مسیرها طی شود، عدم حضور در بازارهای جهانی تولید را مقرون به صرفه نخواهد کرد و هزینه‌های تولید بیشتر از واردات آن خواهد بود. در سال‌های گذشته دولت با حمایت از تولیدکنندگان به حضور آن‌ها در بازارهای جهانی کمک می‌کرد. حمایت از شرکت‌های تولیدکننده برای حضور در نمایشگاه‌هایی چون جیتکس و سبیت در سال‌های پیش توانسته بود کیفیت تولید محصولات داخلی را تا حدود زیادی افزایش دهد، اتفاقی که در سال‌های اخیر کمتر شاهد آن بودیم.

عامل اساسی آسیب‌پذیری کشور در بحث امنیت را در چه زمینه‌ای می‌بینید؟ و برای رفع آن چه راهکاری را پیشنهاد می‌کنید؟

به اعتقاد من اولین اتفاقی که کشور را با آسیب‌های امنیتی مواجه می‌کند، پایین بودن سطح فرهنگ امنیت اطلاعات کاربران است. به عنوان مثال هنوز بسیاری از مدیران ما از کلمه‌های عبوری استفاده می‌کنند که بسیار ساده و غیر ایمن است. قاعدتاً برای رفع چنین مشکلی آموزش کاربران و القای این نکته که حفظ امنیت از اهمیت بالایی برخوردار است، مهمترین راهکار و راه حل است.

با توجه به اظهارات غرب در خصوص ارتش سایبری ایران، دیدگاه شما چیست؟ وجود ارتش سایبری تا چه اندازه در کنترل این گونه حملات کمک می‌کند؟

در طول تاریخ و به ویژه طی سال‌های اخیر، فناوری اطلاعات با دگرگونی و انقلاب روبرو بوده و دستخوش تغییرات بزرگی شده است. در واقع فناوری‌های نوین تبدیل به یک سلاح، منبع انرژی یا یک وسیله ارتباطی جدید شده است که همگی باعث شده است، کشورها از جنگ فرسایشی پرهیز کرده و در عوض با استفاده از این فناوری‌های جدید جنگ‌آوری را متحول کرده‌اند.

امروزه جنگ سایبری و یا ارتش سایبری به دایره لغات اضافه شده‌اند و همانگونه که نیروهای زمینی، هوایی و دریایی جزء لاینفک ارتش‌های جهان شده است، وجود بخش سایبری در هر ارتشی نیز لازم و ضروری است. در «جنگ‌های اطلاعاتی»، حفاظت از اطلاعات نقش اساسی دارد و ارتش سایبری نیز نقش محافظان این اطلاعات را بر عهده گرفته‌اند. بارها مسئولان، از جنگی یاد کرده‌اند که علیه ما در جریان است. ویروس‌ها و بدافزارهایی که روزانه به کشور هجوم می‌روند نیز گواه این ادعا است.

در چنین شرایطی ارتش سایبری می‌تواند به ما در کنترل و مقابله با چنین حملاتی کمک کند. البته جنگ سایبری، جنگی فراگیر است و تک تک افراد جامعه می‌توانند، دروازه‌هایی برای ورود بدافزارها باشند. در این موقعیت فرهنگ‌سازی حفظ امنیت توسط کاربران، عمده‌ترین وظیفه‌ای است که نهادهای حاکمیتی دارند. اگر فرهنگ امنیت اطلاعات حاکم شود، این تهدیدات نیز کمتر و کمتر خواهد بود.

تولید محصول بومی تنها راه مقابله با سلطه سایبری است

بزرگ‌نمایی هر حمله کوچک دشمن به فضای سایبری کشور مشروعیت بخشیدن به عمل آن‌هاست. بهتر است از طریق تقویت زیرساخت‌های امنیتی کشور با تکیه بر دانش فنی بومی در کنار دفاع از سرمایه‌های ملی به دور از بزرگ نمایی‌ها بر افزایش قدرت سایبری خود متمرکز شویم تا بتوانیم زیرساخت‌های حیاتی کشور را از نفوذ بیگانگان مصون بداریم. سردار غلامرضا جلالی، رئیس سازمان پدافند غیرعامل کشور با این اعتقاد، با پایگاه خبری افتانا به گفتگو می‌پردازد که شرح آن را در ادامه می‌خوانید.

جنگ سایبری، دفاع سایبری

مهم‌ترین رویداد حوزه امنیت، حملات سایبری متعددی است که در سال جاری زیر ساخت‌های کشور را مورد تهدید قرار داده و سعی در وارد آوردن خسارت به سرمایه های ملی داشتند. با توجه به اینکه بسیاری از مفاهیم دنیای امروز به فضای سایبری منتقل و سرمایه‌های کشورها تبدیل به سرمایه‌های سایبری شده‌اند، توجه بیشتری به این دست تهدیدات و حملات به فضای مجازی معطوف شده و رویکرد جدیدی نسبت به فضای سایبری کشور در بین مسئولین به وجود آمده و متخصصین بخش‌های دولتی و خصوصی این حوزه را به فعالیت و تمرکز بیشتر بر امر امنیت فضای سایبر وا داشته است.

از زمانی که سرمایه‌های اقتصادی کشورها به سرمایه‌های سایبری تبدیل شدند و مفاهیم حفظ سرمایه و محافظت از سرمایه‌ها و دنبال کردن ارتقاء و پایداری سرمایه‌ها به این فضا منتقل شد شاهد خلق مفاهیمی مانند امنیت و جنگ سایبری بودیم که جنگ سایبری، دفاع سایبری را نیز ایجاب می‌کند.
در چند سال گذشته کشور ما به عنوان هدف، در این فضا چندین مرتبه مورد تهاجم واقع شده و به سرمایه‌های ملی آن حمله و خساراتی وارد آمده است و از آنجا که این سرمایه‌ها به تمام کشور تعلق دارد می‌توان گفت این حملات منافع ملی کشور را تهدید کرده‌اند. در تمام دنیا نیز وقتی تهدیدات در حوزه منافع ملی و حیاتی کشورها باشد، باعث بروز جنگ می‌شود. بنابراین برای تعیین قلمرو در فضای سایبری نیازمند ادبیات جدیدی هستیم که مفاهیم مورد نیاز در فضای سایبر را تعریف کند.

قلمرو سایبری کشورها کجاست

بیرون از فضای سایبری مفهوم «سرزمین» در حوزه دفاع مشخص است و تجاوز واحد نظامی یک کشور به قلمرو سرزمین دیگر باعث بروز جنگ می‌شود. در فضای سایبر نیز نیاز به تعیین قلمرو وجود دارد زیرا نبود مرز و قلمرو در این فضا مشکلاتی ایجاد می کند.

حمله سایبری هدفمندی که از سوی یک کشور برای ورود به زیرساخت‌های حیاتی و تهدید منافع ملی صورت گیرد و وارد حوزه امنیت ملی کشورها شود، این حمله مصداق مشخص جنگ است.

طبق شاخص‌های موجود در حوزه دفاع سایبری هر نوع حمله‌ای به منظور جنگ تلقی نمی‌شود و جنگ در این حوزه ملاک‌های شناسایی مشخصی از جمله: سطح، منشاء، حوزه تولید خطر و وسیله حمله دارد. حمله یک فرد یا یک گروه مثلا یک گروه تروریستی و یک کشور و حمله به یک سایت اطلاع رسانی کم اثر یا زیر ساخت‌های حیاتی و حساس کشورها سطوح متفاوتی از دفاع سایبری را ایجاب می‌کند، همچنین در این مقوله سلاح مورد استفاده نیز نقش مهمی دارد.

بین استفاده از سلاح سایبری و یک ویروس معمولی تفاوت‌هایی وجود دارد. در سلاح‌های تولید شده نیز چند ویژگی شامل: میزان پیچیدگی، لایه های رمز شوندگی ویروس، فرمان پذیری ویروس، قابلت پنهان شوندگی، قابلیت ارسال و جمع‌آوری و قابلیت خودکشی مورد توجه است که یک ویروس معمولی را از یک سلاح سایبری متفاوت می کند. مثلا زمانی که استاکس نت شناسایی شد تمام متخصصین این حوزه نتیجه گرفتند که این ویروس یک ویروس معمولی نیست بلکه یک سلاح سایبری است.

با توجه به اینکه مدیریت زیر ساخت‌های حیاتی در فضای سایبر قرار می‌گیرد حوزه امنیت و جنگ در فضای سایبری باید به صورت لایه‌ای تعریف شود. اولین تعریف این است که با حمله به سامانه های مدیریتی

تهدید شکل می‌گیرد. همچنین لازم است نقش تمامی دستگاه های اجرایی از جمله وزارتخانه‌های دفاع، اطلاعات، ارتباطات و پلیس فتا با تدوین دستورالعمل مشارکت آن‌ها در مقوله دفاع سایبری با محوریت سازمان پدافند غیرعامل مشخص شود.

تعیین حد و حدود و قلمرو در فضای سایبری مسئله‌ای است که توجه سیاستمداران کشورهای مختلف را به خود جلب کرده است. برای شناخت حد و مرزها در فضای سایبر لازم است تا ادبیات لازم برای شناخت شاخص‌های این حوزه تدوین شود. در این راستا سازمان پدافند غیر عامل کشور با هدف تدوین ساز و کار دفاع در برابر تهدیدات و تدوین ادبیات مورد نیاز این حوزه تشکیل شد. تا با انجام تحقیقات گسترده ای دراین حوزه با تلفیق ادبیات نظامی، ادبیات استراتژیک و ادبیات سیاسی استراتژیک به تعیین حد و حدود و قلمرو کشور در فضای سایبر بپردازد.

تولید دانش فنی، مهم‌ترین نیاز امنیتی کشور

در اولین قدم این سازمان با همکاری سازمان‌های مختلف از جمله وزارت دفاع، وزارت ارتباطات، وزارت اطلاعات سعی دارد با تعریف شاخص‌های امنیت در سه سطح فردی، اجتماعی و ملی مشخص کند که چه سطحی از امنیت، دفاع نامیده می‌شود. در واقع طبق تعریف موجود امنیت در سطح فردی ایمنی در سطح گروهی امنیت عمومی و اجتماعی و در سطح ملی دفاع نامیده می‌شود.

نخستین مشکل کشور در مقوله امنیت سایبری این است که ابزار، الفبا، متدولوژی، قوانین و محصولات مورد استفاده را تولیدات خارجی تشکیل می‌دهند. واضح است که تولیدکننده یک محصول امنیتی تمام راه‌های نفوذ آن را می‌شناسد پس به چنین محصولی در سطوح بالا و حساس امنیتی نمی‌توان اعتماد کرد. برای سطوح پایین‌تر شاید بتواند مورد استفاده قرار گیرد اما در مورد زیر ساخت‌های حیاتی که امنیت ملی را در بر می‌گیرد استفاده از این ابزارها، خطرناک‌تر از نبود ابزار امنیتی است. بنابراین لازم بود تا رویکرد جدیدی به حوزه دفاع در بین مسئولین و متخصصین این امر پدید آید.

در راستای این هدف برنامه ای جهت تولید محصولات بومی با تلفیق چند دانش از جمله علوم نظامی، استراتژیک سایبری و فنی سایبری در دستور کار قرار گرفت. تا محصولاتی انحصاری، ابتکاری، بومی، عمیق، لایه به لایه و هوشمند در حوزه دفاع سایبری تولید شود. یعنی مدلی از دفاع تدوین شود که کاملا در انحصار ما با شد و نمونه آن وجود

نداشته باشد. نرم افزار بومی محصولی است که در داخل کشور طراحی، کدنویسی و تمام اجزاء آن تعریف شده باشد.

بنابراین نیاز به صنعت دفاع سایبری داریم تا بتوانیم همانند دیگر حوزه‌های دفاعی که متکی بر سلاح‌های بومی هستند ابزار مورد نیاز دفاع سایبری بومی را نیز تولید کنیم. در این خصوص از اساتید و متخصصان حوزه امنیت سایبری دعوت شد تا جهت فراهم کردن دانش مورد نیاز برای تولید محصولات امنیتی بومی محتوا ارائه دهند. پس از بررسی نتایج متوجه این مسئله شدیم که دانش فنی موجود در کشور اندک است و به عنوان اولین گام لازم است که دانش داخلی تقویت شود.

نرم‌افزار بومی یعنی محصولی که در داخل کشور طراحی، کدنویسی و تمام اجزاء آن تعریف شده باشد چنین محصولی مسلما برای ایجاد امنیت قابل اعتماد تر است.

به عنوان اولین گام درجهت دستیابی به این هدف دوره‌های کارشناسی ارشد دفاع سایبری در دانشگاه های امام حسین و مالک اشتر برای ترم جاری و دکترا برای ترم آینده در دانشگاه دفاع با محوریت استاد تدوین شدند؛ و هماهنگی‌هایی بین پلیس فتا، وزارت خارجه و قوه قضائیه برای تدوین دکترین دفاع حقوقی صورت گرفت.

یکی دیگر از اشکالاتی که وجود دارد این است که سامانه تهدیدات حملات را بعد از وقوع آن‌ها تشخیص می‌دهد. بنابراین نیاز به طراحی سامانه ای جهت پایش، رصد، تشخیص و هشدار به موقع تهدیدات مطرح گردید. زیر ساخت‌های فنی و ستادی این سامانه با نظارت شورای عالی امنیت ملی فعال شده و در حال توسعه است تا بر روی حملات سایبری تجزیه و تحلیل انجام دهد و قبل از بروز خسارت تهدیدات را شناسایی کند.

قدرت سایبری یا ارتش سایبری ...

ما معتقدیم که به جای اینکه در پی دستیابی به ارتش سایبری باشیم بهتر است به قدرت سایبری دست پیدا کنیم زیرا در دانش و فناوری در این حوزه در حال فراگیر شدن است و شرایط چند کارکردی و دانش‌های مختلف بین رشته ای را ایجاد می‌کند و تکنولوژی در حال حل شدن در فضای سایبری است.
بنابراین بهتر است که مولفه‌های قدرت آینده کشور را بشناسیم. بالاترین قدرت در کشور منابع انسانی است بنابراین لازم است سعی در تولید منابع انسانی با کیفیت داشته باشیم.

خود کفایی و استقلال در بخشی از زیرساخت‌های امنیتی مهم‌ترین مقوله قدرت سایبری است که نیاز به وجود استراتژی و صنعت جدی در این حوزه دارد. پس بهتر است که مرکز دفاع سایبری قدرتمندی داشته باشیم تا حملات دشمن را کنترل کند و قدرت پاسخ‌گویی به حملات و دفاع مشروع را نیز داشته باشد.
سامانه فرماندهی و کنترل باید بتواند مدیریت استراتژی و اطلاع رسانی داشته باشد تا در کنار ایجاد آرامش از طریق اطلاع رسانی صحیح عکس العمل های درست و دقیق از خود نشان دهد.

روابط عمومی و مشاوره رسانه‌ای

دیده‌بان آی‌تی، دیده‌بان فرصت‌های نو

www.didehban.com
info@didehban.com
تلفن: ۸۸۷۴۹۴۱۰ فکس: ۸۸۷۴۹۴۱۵
تنها موسسه روابط عمومی در حوزه آی‌تی در ایران

وضعیت نشت اطلاعات در جهان

بخش هایی که بیشترین نشت اطلاعات در آن اتفاق می افتد

کشورهایی که بیشترین نشت اطلاعات در آن‌ها اتفاق می افتد

۷۸%

درصد شرکت‌های حاضر در فهرست فوربس ۲۰۰۰ که احتمال نشت در وب سایت‌هایشان وجود دارد و فرم‌های حاوی اطلاعات مفیدشان در معرض خطر است.

۱۵%

درصد شرکت‌های حاضر در فهرست فوربس ۲۰۰۰ که به هکرها اجازه دسترسی به وب سایت‌ها را به منظور آزمایش می‌دهند و امکان ورود به پرتال‌ها و آپلود فایل‌هایشان وجود دارد.

۷۱%

درصد شرکت‌های حاضر در فهرست فوربس ۲۰۰۰ که از نسخه‌های قدیمی نرم‌افزارهای مایکروسافت و ادوبی استفاده می‌کنند و احتمالا در معرض خطر هستند.

منبع: KPMG

clavister®

ناظر دقیق و قابل اعتماد با عملکردهای فوق العاده در امنیت شبکه

560 Gbps

سریعترین UTM جهان

www.clavister.com

- تنها تولید کننده فایروال UTM صنعتی
- تکنولوژی کشور سوئد
- سیستم‌های عامل منحصر به فرد cOS Stream, cOS Core

تجارت امن
FORTIFY YOUR IT SECURITY

توزیع کننده انحصاری محصولات کلاویستر در منطقه خاورمیانه
تلفن: ۳-۸۸۱۹۰۶۴۱ / www.tejarateamn.com / info@tejarateamn.com

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