

می‌گوید: «برخی ممکن است به دلایل علمی از VPN استفاده کنند و برخی دیگر به دلایل کاری. مثلاً افرادی برای اتصال به کتابخانه دانشگاه‌شان از VPN استفاده می‌کنند و بعضی از یک محیط آزمایشگاهی مبتنی بر VPN برای انجام یک کار علمی-تحقیقاتی بهره می‌برند. در کسب‌وکارها، برخی از VPN برای اینکه دفاتر مختلف شرکت‌شان را به یکدیگر متصل کنند یا مثلاً به یک سازمان بالادستی وصل شوند تا بتوانند آن استعمال بگیرند، استفاده می‌کنند. وقتی روی VPN ها اختلال ایجاد شود، ارتباطات همه اینها دچار مشکل می‌شود. اگر هم اختلالی به وجود نیاید، نمی‌توان با فیلترشکن مبارزه کرد. پس ترجمه این عبارت گنگ «باید با فیلترشکن مبارزه شود»، می‌شود خراب شدن ارتباطات رمزنگاری شده که برای عملکرد عادی و سالم شبکه و فعالیت کسب‌وکارها، مراکز تحقیقاتی و... نیازی ضروری است.»

▼ کوتاه آمدن از استانداردهای امنیتی

اختلالاتی که روی ارتباطات رمزنگاری شده رخ می‌دهد، می‌تواند به نحوی روند فعالیت را با مشکل مواجه کند که برخی از کسب‌وکارها ناچار شوند از استانداردهای امنیتی خود کوتاه بیایند تا بتوانند فعالیت‌شان را ادامه دهند. سعید سوزنگر، مدرس شبکه و امنیت و کنشگر حقوق دسترسی دیجیتال نیز با تأکید بر اینکه VPN‌ها ذاتاً باعث افزایش امنیت می‌شوند، به هم‌میهن می‌گوید: «زمانی که درباره انواع تانلینگ یا روش‌های تانل زدن و VPN و موارد این‌چنینی صحبت می‌کنیم، داریم درباره راهکار امنیتی حرف می‌زنیم. اما راه دستیابی به ابزارهای مطمئن هم خود یک مسئله است. افرادی هستند که VPN‌های آلوده‌ای را توسعه می‌دهند و منتشر می‌کنند یا در تلگرام می‌گذارند و می‌گویند افراد فایل apk را دانلود کنند. اینها ابزارهای دستکاری شده هستند که ممکن است باعث بشوند یکسری از اطلاعات شخصی کاربر نشت پیدا کند، ولی اینها درصد بسیار کمی هستند.»

سوزنگر تأثیری را که افزایش استفاده از فیلترشکن‌ها روی شبکه می‌گذارد، منحصر به استفاده از فیلترشکن‌های آلوده نمی‌داند و با اقبال در خصوص اثرگذاری سیاست مبارزه با فیلترشکن روی کسب‌وکارها هم‌نظر است و چنین توضیح می‌دهد: «به خاطر مسئله فیلترینگ ما مجبور می‌شویم از ابزارهای تانلینگ و VPN استفاده کنیم و سربار شدیدی را به شبکه تحمیل می‌کنیم، زیرا حق‌مان را می‌خواهیم و لازم است به اینترنت بدون فیلتر دسترسی داشته باشیم. بعد از اینکه این سربار روی شبکه ایجاد شد، حاکمیت روی آن اختلالاتی ایجاد می‌کند و خیلی از کسب‌وکارها در میانه نبرد بین حاکمیت و کاربر برای فیلتر کردن و دور زدن فیلترینگ قرار می‌گیرند. این اتفاق باعث می‌شود روی پروتکل‌های امنیتی و رمزنگاری که ذاتاً وظیفه ایمن‌سازی را برعهده دارند، اختلال باشد و صاحب کسب‌وکار بعضاً ناچار می‌شود این پروتکل‌ها را روی شبکه‌های خود غیرفعال کند. یعنی من نوعی که در حال پیش‌بردن کسب‌وکاری هستیم، برای اینکه چرخش بچرخد، به خاطر اختلال‌هایی که روی پروتکل‌ها هست، این پروتکل‌ها را غیرفعال می‌کنم و سرویس‌هایم را از لحاظ امنیتی تقلیل می‌دهم که این باعث ناامنی می‌شود و نشت اطلاعات و موارد این‌چنینی را سبب خواهد شد.»

این مدرس شبکه و امنیت با مثالی توضیح می‌دهد که چگونه این اختلالات می‌توانند ساده‌ترین فعالیت‌های یک کسب‌وکار را با مشکل روبه‌رو کنند و او را به عقب‌نشینی از استانداردهای امنیتی خود وادار سازند؛ «سرورها در دیتاستر قرار دارند. ما صدها هزار سرور در کشور داریم که مدیران هیچ‌کدام در دیتاسترها مستقر نیستند و از راه دور به آن وصل می‌شوند. وقتی روی پروتکلی مثل SSH (SSH مخفف Secure Shell و یک پروتکل شبکه‌ای است که برای برقراری ارتباط امن بین دو دستگاه از آن استفاده می‌شود) اختلال ایجاد می‌شود، من از راه دور نمی‌توانم به آن سرور در دیتاستر وصل شوم. به همین دلیل پروتکلی را با امنیت کمتر فعال می‌کنم که رویش اختلال نیست و به این روش به سیستم وصل می‌شوم و کارهایم را انجام می‌دهم. حتی همین شرایط را برای کاربرانم فراهم می‌کنم تا با یک سطح امنیتی پایین‌تر وصل شوند. چرا؟ چون حاکمان ما روی پروتکلی که نمی‌دانند چیست و رمزنگاری است و فکر می‌کنند کاربرد فیلترشکن دارد، اختلال ایجاد کرده‌اند. کسب‌وکار هم از استانداردهای امنیتی خود کوتاه می‌آید تا فقط سرویسش بالا باشد و کار کند و کاربران بتوانند از آن استفاده کنند.»

▼ خطر فیلترشکن‌های آلوده

آرین اقبال خطر استفاده مردم از فیلترشکن‌های بی‌نام‌ونشان و آلوده را جدی‌تر می‌داند و می‌گوید از آنجا که مردم برای زیست روزمره خود هم به ابزار فیلترشکن نیاز دارند، چنانچه آگاهی لازم را نداشته باشند، ممکن است به داندلود و نصب فیلترشکن‌های

آلوده اقدام کنند که خود این مسئله می‌تواند زمینه‌ساز اتفاقات دیگر باشد. او در این باره توضیح می‌دهد: «با افزایش فیلترینگ، عموماً چاره‌ای جز استفاده از ابزار فیلترشکن وجود ندارد. شاید برای شرکت‌ها و متخصصان حوزه کامپیوتر امنیت فیلترشکن مهم باشد، ولی بیشتر مردم از هر چیزی که کار کند، استفاده می‌کنند. حالا ممکن است آن را از موبایل فروش سر کوجه خریده باشند یا همین طوری از تلگرام داندلود کرده باشند. اینجاست که قضیه خطرناک می‌شود. اگر از یک فیلترشکن شناخته‌شده بین‌المللی، مثل VPN‌های معروفی که به‌صورت رایگان یا در ازای خرید اشتراک در اختیار افراد قرار می‌گیرند، استفاده شود، هیچ مشکلی وجود ندارد. دسترسی‌ها در این VPN‌ها فقط در حدی است که شاید مالک آن بتواند آمارهایی کلی از اینکه کاربران کدام کشورها با این VPN بیشتر از چه سایت‌هایی بازدید می‌کنند، ارائه دهد. زیرا تمام ارتباطات ما حتی داخل VPN باز هم رمزنگاری شده است. درنتیجه حتی داخل VPN هم ترافیک ما قابل دیدن نیست. اما مسئله فیلترشکن‌های بی‌نام‌ونشانی که مشخص نیست چه کسی، کجا آن را ساخته، متفاوت است.»

آرین اقبال کنشگر اینترنت آزاد: **با افزایش فیلترینگ، عموماً چاره‌ای جز استفاده از ابزار فیلترشکن وجود ندارد. شاید برای شرکت‌ها و متخصصان حوزه کامپیوتر امنیت فیلترشکن مهم باشد، ولی بیشتر مردم از هر چیزی که کار کند، استفاده می‌کنند.** اینجاست که قضیه خطرناک می‌شود. اگر از یک فیلترشکن شناخته‌شده بین‌المللی، مثل VPN‌های معروفی که به‌صورت رایگان یا در ازای خرید اشتراک در اختیار افراد قرار می‌گیرند، استفاده شود، هیچ مشکلی وجود ندارد. دسترسی‌ها در این VPN‌ها فقط در حدی است که شاید مالک آن بتواند آمارهایی کلی از اینکه کاربران کدام کشورها با این VPN بیشتر از چه سایت‌هایی بازدید می‌کنند، ارائه دهد. زیرا تمام ارتباطات ما حتی داخل VPN باز هم رمزنگاری شده است. درنتیجه حتی داخل VPN هم ترافیک ما قابل دیدن نیست. اما مسئله فیلترشکن‌های بی‌نام‌ونشانی که مشخص نیست چه کسی، کجا آن را ساخته، متفاوت است.»

درنهایت اینکه فیلترینگ گسترده، نیازی را در بازار ایجاد کرده که گاهی پاسخ به این نیاز سالم است و گاه آلوده و می‌تواند ابزاری به دست هکرها بدهد که یا از خود کاربران دزدی کنند یا از سیستم این کاربران برای حمله کردن به جاهای دیگر و از کار انداختن سرویس‌ها بهره گیرند.

▼ فیلترینگ هرگز راه‌حل نیست

با تغییر دولت و به تبع آن، وزیر ارتباطات، برخی امیدوارند بتوانند گره کور فیلترینگ را باز کنند. در این

میان اتحادیه‌ها و سازمان‌هایی که از منافع و حقوق

صنف فناوری اطلاعات دفاع می‌کنند، بارها ناکارآمدی

و زیان‌بار بودن سیاست فیلترینگ را متذکر شده‌اند.

بهناز آریا که مدت‌هاست ریاست کمیسیون افنا (امنیت فضای تولید و تبادل اطلاعات) را در سازمان نظام صنفی رایانه‌ای استان تهران برعهده دارد، درباره تأثیرات فیلترینگ و راهی که طی این سال‌ها پیموده‌اند به هم‌میهن می‌گوید: «سازمان نظام صنفی از روزی که اولین فیلترینگ روی موارد پرکاربرد در حوزه فناوری اطلاعات اتفاق افتاد، دائماً نظرات خود را در جلسات مختلف به متولیان امر اعلام کرده است؛ زیرا فیلترینگ تأثیرات گسترده‌ای دارد و مشکلات بسیاری را پیش آورده است. بخشی از مشکلات مسئله فیلترینگ به استفاده آحاد مردم برمی‌گردد و کاربردی که آن پلتفرم‌ها و اپلیکیشن‌های فیلترشده برایشان دارد. اما بخش دیگر اثرات فیلترینگ، تخصصی‌تر و مرتبط با کسب‌وکارهاست. دسترسی شرکت‌هایی که در صنعت فناوری اطلاعات فعالیت می‌کنند، به یکسری از موارد حیاتی با معضل مواجه شده است. مشکلات عدیده امنیتی و افزایش آسیب‌پذیری‌ها مشکلات کسب‌وکارها را چند برابر کرده است. حتی در مواردی با توجه به فیلترینگ دسترسی برای به‌روزرسانی برخی تجهیزات بسته می‌شود و همین عاملی برای مضاعف شدن مشکلات امنیتی خواهد بود. به همین دلیل هم سازمان نظام صنفی از همان ابتدا به‌صورت فعالانه نظر خود را در مورد فیلترینگ اعلام کرده، به‌خصوص در یکی، دو سال اخیر که فیلترینگ و استفاده از فیلترشکن‌ها گسترده‌تر شده است.»

او نیز فیلترشکن‌های غیراستاندارد و بدون نام‌ونشان را معضل مهمی می‌داند و تأکید می‌کند: «در حال حاضر ما با تعداد زیادی فیلترشکن بی‌نام‌ونشان مواجهیم که می‌توانند مشکلات بسیاری را ایجاد کنند. متأسفانه به‌دلیل اینکه فیلترینگ دسترس‌پذیری

را پایین می‌آورد، کاربر نهایی به تنها چیزی که فکر می‌کند، بالا بردن دسترس‌پذیری خود است و به‌هیچ‌وجه به محرمانگی اطلاعاتش نمی‌اندیشد و همه دسترسی‌ها را روی سیستم‌های خود به فیلترشکن می‌دهد. این فاجعه‌بار است. به همین دلیل نظر ما این بوده که فیلترینگ هرگز راه‌حل نیست.»

به گفته آریا، سازمان نظام صنفی رایانه‌ای درخصوص فیلترینگ و آسیب‌هایی که این روش به کسب‌وکارها وارد می‌کند، طی این سال‌ها با بسیاری از متولیان امر صحبت کرده‌اند؛ سازمان فناوری اطلاعات، افتای ریاست‌جمهوری، مرکز ملی فضای مجازی، وزارت ارتباطات و...: «نه‌تنها ما در کمیسیون افتای نظام صنفی، بلکه سایر بخش‌ها و کمیسیون‌ها نیز در جلسات خود مکرراً این مسائل را در جلسات با متولیان مطرح کرده‌اند. متأسفانه تصمیم‌گیری در این حوزه در سطح بالایی اتفاق می‌افتد و کسانی که با آنها جلسه برگزار می‌کنیم، تصمیم‌گیر نهایی در این خصوص نیستند.»

رئیس کمیسیون افتا می‌افزاید: «ما حتی سعی کردیم سراغ موضوعات تخصصی‌تر برویم که نیازهای افرادی چون توسعه‌دهندگان تأمین شود یا تجهیزات بتوانند به‌روزرسانی شوند. بارها مطرح کردیم که حداقل از گوگل‌پلی رفع فیلتر شود. با این وجود به نتیجه نرسیدیم و تا الان هیچ‌کدام از این مذاکرات به نظر من موفقیت‌آمیز نبوده است.»

آریا درساره راه‌حل‌های جایگزین پیشنهادی می‌گوید: «ما همواره در این سازمان بر این عقیده بوده‌ایم که روش‌های حذفی و پاک کردن صورت‌مسئله پاسخگو نیست و ما باید سراغ راه‌حل‌هایی برویم که دسترس‌پذیری را با این سطح از اختلال مواجه نکند. از آموزش دادن و آگاهی‌رسانی درخصوص آسیب‌های احتمالی پلتفرم‌ها گرفته تا ارائه جایگزین‌های جذابی که مردم به‌شکل خودخواسته به‌جای پلتفرم‌های خارجی از آنها استفاده کنند. اینها پیشنهادهایی بوده که در جلسات خود بارها آنها را مطرح کرده‌ایم.»

او از دولت جدید انتظار دارد حداقل صدای بخش خصوصی را به گوش تصمیم‌گیران برساند و درباره جلسه‌ای که چندی پیش با وزیر ارتباطات دولت چهاردهم داشته‌اند، می‌گوید: «در جلسه‌ای که با آقای ستار هاشمی داشتیم هم این موضوع را مطرح کردیم و او نیز معتقد بود، وضعیت فعلی مطلوب نیست. طبیعتاً موضوع امنیت ملی اولویت همه ما، چه در بخش خصوصی و چه در حاکمیت است، اما این امنیت می‌تواند به نحوی تأمین شود که کمترین مشکل را ایجاد کند. درست است که درباره موضوع فیلترینگ در سطح بالاتری از دولت تصمیم‌گیری می‌شود، اما حداقل انتظاری که داریم این است که دولت صدای بخش خصوصی باشد، با ما همراهی کند، شرایط واقعی حاکم بر صنعت را ببیند و به افراد و نهادهای تصمیم‌گیر منتقل کند. بالاخره این صنعت فناوری اطلاعات باید حداقل‌هایی را داشته باشد تا بتواند فعالیت اقتصادی و فناورانه انجام دهد. چیزی که در شرایط فعلی بسیار سخت شده است. موضوعی که با وزیر ارتباطات مطرح کردیم هم همین بود که حداقل با ما همراهی کند و در مواردی که ممکن است صدای ما باشد تا بتوانیم به راه‌حلی برسیم که هم ملاحظات امنیتی مدنظر حاکمیت رعایت شود و هم صنعت بتواند به حداقل‌هایی که برای توسعه‌اش لازم است، دسترسی داشته باشد.» آریا تأکید می‌کند که به روال گذشته به‌صورت موازی با سایر متولیان حوزه نیز همچنان مذاکرات خود را ادامه می‌دهند تا به راه‌حلی برسند که از شرایط نامطلوب فعلی خارج شویم.

▼ سیاستی در تضاد با امنیت

داده‌ها نشان می‌دهند سیاست‌های حاکمیت برای مبارزه با فیلترشکن‌ها بی‌هوده و ناکارآمد بوده و بار دیگر ثابت می‌کنند سیاستی که بدون داشتن حمایت اکثریت، می‌خواهد از طریق زور و اجبار جامعه را با خود همراه کند، قطعاً شکست‌خورده است. وب‌سایت‌ها و اپلیکیشن‌هایی که به بهانه تأمین امنیت ملی زیر تیغ تیز فیلترینگ قرار گرفته‌اند، بعید است می‌توانستند به اندازه‌ای که جدال میان فیلترشکن‌ها و سیاست مبارزه با آن به امنیت ملی آسیب زده‌اند، به ما ضربه وارد کنند. هر چند تغییر دولت، به‌دلیل اینکه این سیاست از دست دولت‌ها خارج است، احتمالاً نتواند به‌شکل مستقیم مسئله فیلترینگ را حل‌وفصل کند، اما همراهی دولت با مردمی که خود را نماینده آنها می‌داند و از این وضعیت در سطوح مختلف به تنگ آمده‌اند، شاید راهگشا باشد.

استفاده از عبارات کلی مانند «استفاده مردم از فیلترشکن‌ها امنیت شبکه را کاهش می‌دهد»، آن هم از سوی سیاست‌گذاران فناوری، بدون آنکه به سازوکار و چرایی آن بپردازند، آدرس‌دهی غلطی است که به‌جای حل مشکل، باز هم می‌خواهد «مردم» را به‌عنوان عامل مشکلات نشان دهد و قسمتی دیگر از پازل پاک کردن صورت‌مسئله به‌جای حل مسئله است.

عدالت فناوری

آموزش مطلوب اقتصاددیجیتال



محمدهسین انصاری توسعه‌دهنده استعدادها

عمده‌ی مشاغل اقتصاد دیجیتال چه در ایران و چه در جهان، بیشتر از آن‌که علم‌محور باشند، تجربه‌محور (Practice Based) هستند. یعنی بیشتر از آن‌که به دانشگاه و دروس نظری نیاز داشته باشند، به محلی برای مواجهه‌ی واقعی با مسئله‌ی آن شغل نیاز دارند و کسی که بتواند تجربه‌ی حل مسئله در اختیارشان بگذارد.

امر یادگیری در این مشاغل نیز، به همین صورت مختصات متفاوتی دارد. ما نیازمند شیوه‌هایی از یادگیری هستیم که شیب یادگیری را نه‌با درس نظری، بلکه با فراهم کردن فرصتی از تجربه کم کند. این‌جاست که نقش بنگاه‌های فناوری از دانشگاه‌ها و مراکز آموزشی مهم‌تر می‌شود. درواقع اگر ما شرکت‌های خصوصی می‌خواهیم که نیروی کار به‌سرعت وارد بازار کار شود لازم است که خودمان آستین بالا بزنیم و آموزش‌هایی مبتنی بر تجارب شغلی مدنظرمان تولید کنیم و هم‌زمان فرصتی برای کارآموزی و شاگردی کردن مهیا سازیم.

اما در شرکت‌های فناوری که زیرساخت آموزشی ندارند، چطور می‌توانیم به این مهم دست‌یابیم؟ یکی از مهم‌ترین شایستگی‌ها و مهارت‌هایی که می‌توان در مسیر رشد نیروهای سازمان از افراد خبره‌ی سازمان انتظار داشت «توسعه‌ی دیگران» است. این شایستگی می‌گوید که فرد خبره چقدر نسبت به آموزش و توسعه دیگران اهمیت می‌دهد و چقدر دانش و توانمندی خود را در جهت تکثیر آن به خدمت می‌گیرد. فرد خبره باید توانمندی و ظرفیت آموزش‌پذیری را در خود توسعه دهد، این ظرفیت شامل پاسخگو بودن، تشویق دیگران به یافتن پاسخ‌ها تا منتقل کردن فوت‌وفن دیگران (Know-how) و حتی نیازسنجی و تنظیم برنامه‌های آموزشی می‌شود.

در مدل‌های جدید شرکت‌داری، تعریف این شایستگی و پیگیری آن از خبرنگان سازمانی برعهده‌ی واحد نیروی انسانی است. این‌که اولاً تعریف مناسبی از این شایستگی در سازمان ارائه دهد و بعد اینکه ظرفیت ایجاد شده را در جهت توسعه‌ی تازه کارها و کارجوها به خدمت بگیرد. هم‌زمان نیز، در سازوکارهای جذب و استخدام، تعریف دو مدل شغلی کارآموزی (Internship) و کارورزی (Apprenticeship) برای مشاغل تخصصی و روبه‌رشد نیز ضروری است. این‌که به‌همراه هر فرد خبره در هر سازمان، دست‌کم یک یا دو کارآموز در سازمان حضور داشته باشند. این اینستکار علاوه‌بر اینکه باعث می‌شود بار یک‌سری از وظایف از دوش خبرنگان کم شود، خیال سازمان را از جانشین‌پروری راحت می‌کند. هم‌زمان هم گستره‌ی زیادی از کارجویان را با آموزشی واقعی، مؤثر و کوتاه‌وارد بازار کار حرفه‌ای می‌کند. در بلندمدت نیز، تأثیر برندی آن چشمگیر خواهد بود.

نوع دیگری از آموزش که سازمان‌ها می‌توانند دنبال کنند، عمومی کردن چالش‌ها، مسائل و دغدغه‌های تخصصی خود در کنار آموزش است. به این صورت که هر فرد بعد از اینکه یک دوره‌ی آموزشی را به پایان رساند، بتواند یک چالش واقعی را حل کند و برای حل آن چالش و ارزیابی نتیجه‌ی آن مربیگری از افراد خبره‌ی سازمان بگیرد. این مدل می‌تواند در مقیاس‌های چندصد نفره و به صورت مداوم تکرار شود. مزیت آن برای سازمان این است که مسائل تخصصی خود را با ذهن‌های تازه یک‌بار دیگر نگاه می‌کند و محلی برای شناسایی افراد با استعداد خواهد بود.

فراموش نکنیم که با مشارکت یک یا دو شرکت در این ابتکارها، اتفاق خاصی در جامعه نمی‌افتد. ما نیازمند یک حرکت جمعی و حضور پررنگ شرکت‌های اقتصاد دیجیتال ایران در کنار هم‌دیگر هستیم. با این حرکت شاید بتوانیم شاهد ایجاد یک اتفاق شگرف در توانمندسازی بازارکار باشیم؛ اتفاقی که منجر به توسعه‌ی اقتصاد دیجیتال می‌شود و این یک روزی روایت توسعه‌ی ما در ایران خواهد بود.