گزارش نظرسنجی افتانا در خصوص

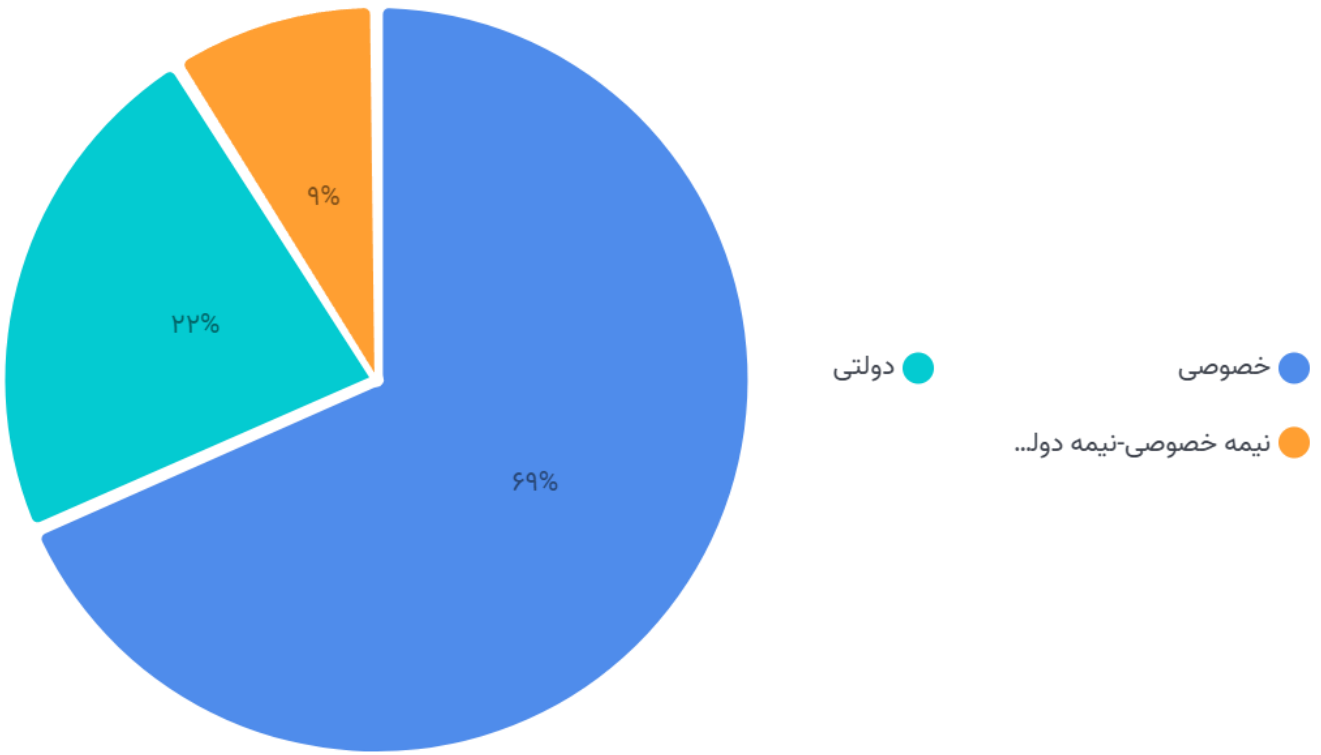
تشکیل ستاد هماهنگی پیشرفت و امنیت فضای سایبری

خبر تشکیل ستاد هماهنگی پیشرفت و امنیت فضای سایبری زیر نظر ریاست جمهوری را می‌توان یکی از اخبار مهم و شاید تعیین‌کننده در آینده افتای کشور دانست. از همین رو افتانا بر آن شد تا به‌جای تعریف و تمجید این اقدام و یا انعکاس نظرات معدودی از کارشناسان؛ در یک نظرسنجی، جویای آرای فعالان حوزه امنیت شود.

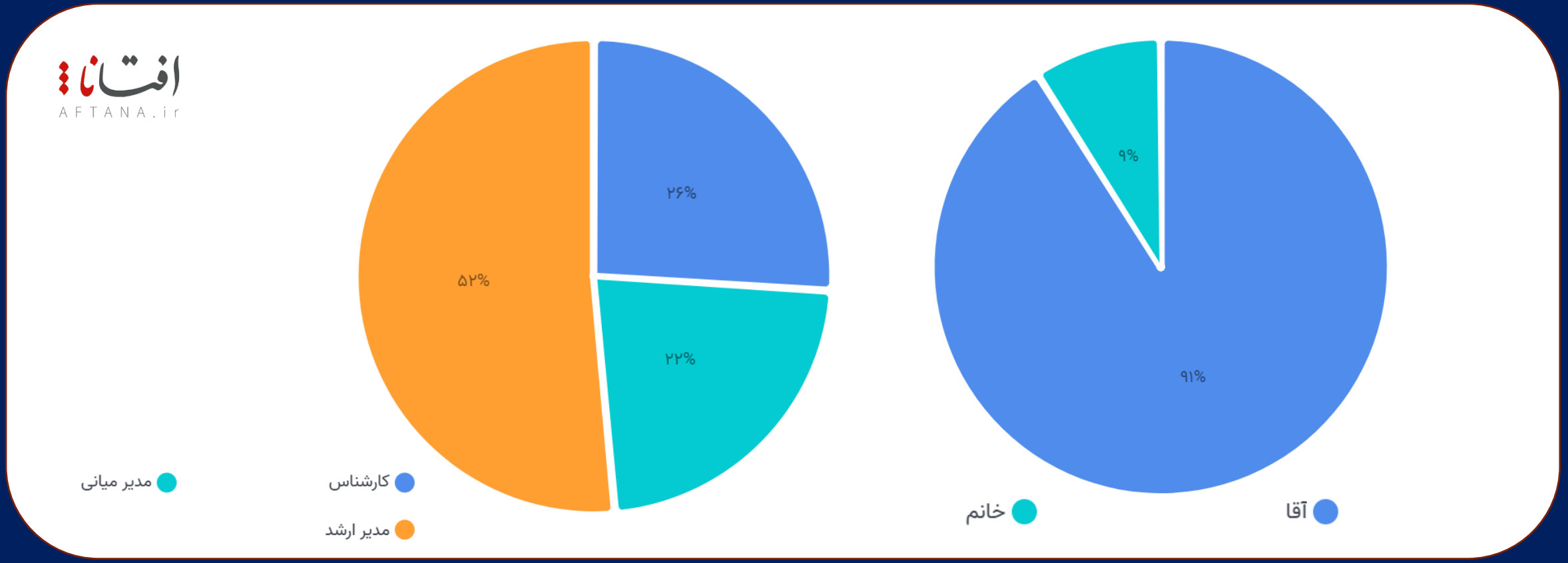
این نظرسنجی از ۲۹ مهرماه به مدت ۵ روز در سایت افتانا فعال بود که در مجموع ۲۵۴ پاسخ دریافت شد. در ادامه نتایج آن را ملاحظه می‌کنید.

سئوال نخست این بود که به‌عنوان یک فعال بخش خصوصی اعلام نظر می‌کنید یا دولتی یا نیمه دولتی.

که دیده می‌شود نزدیک به ۷۰درصد از پاسخ دهندگان از بخش خصوصی هستند.



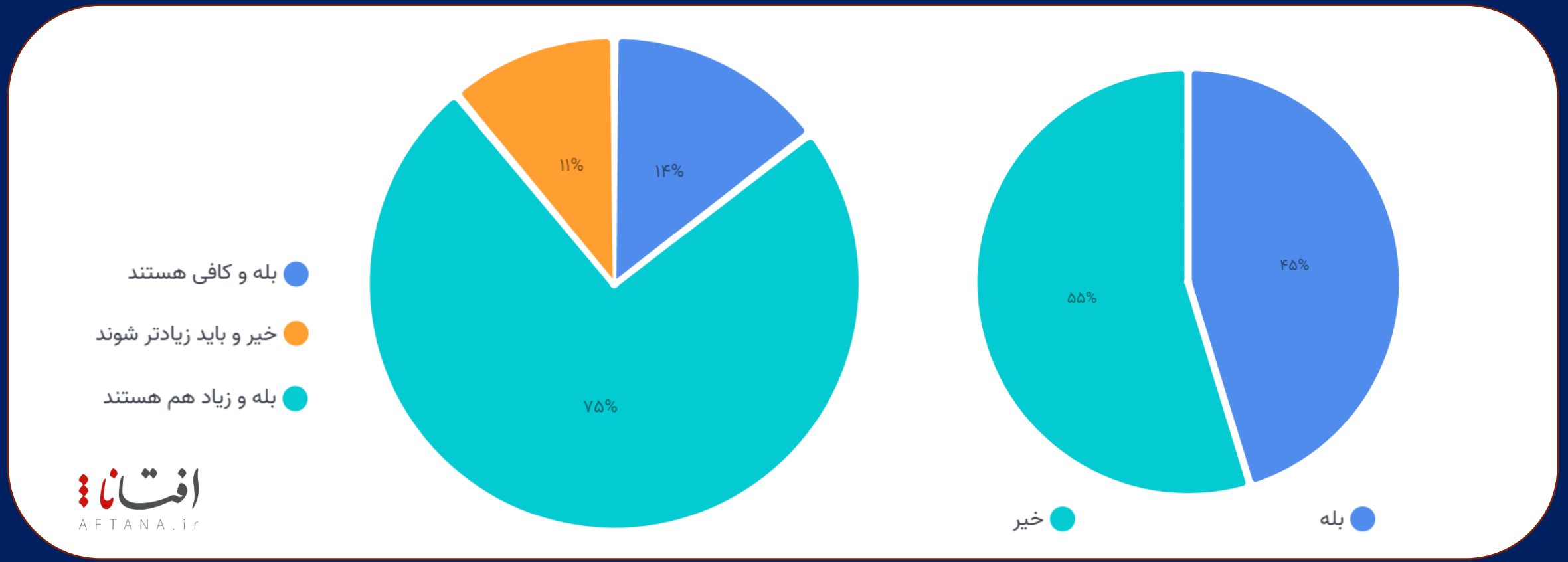
سئوال بعدی به جنسیت پاسخ دهندگان و سمت شغلی آن‌ها مربوط بود. دیده می‌شود که اغلب آقا و در رده مدیران ارشد سازمان هستند.



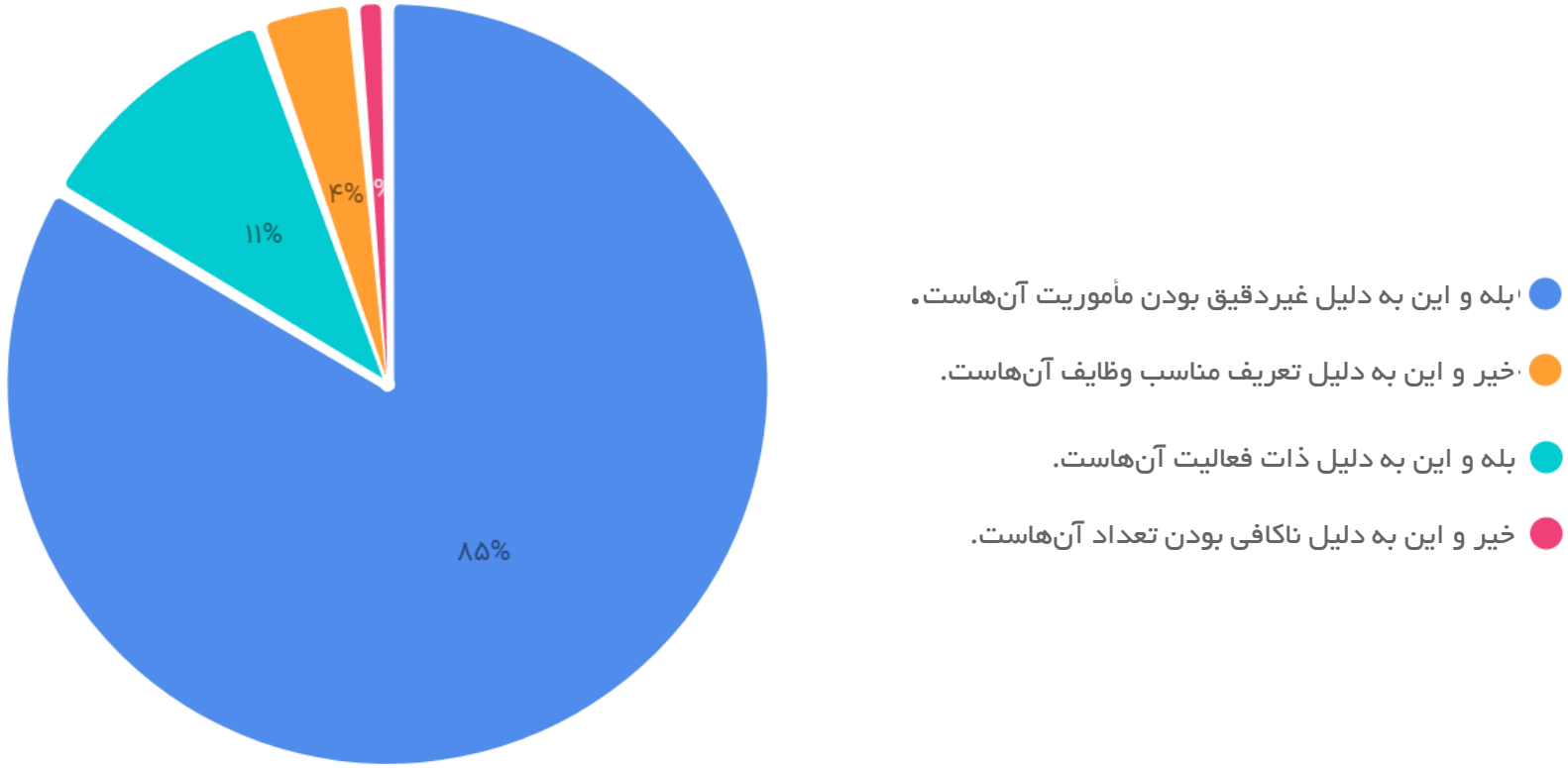
پاسخ دهندگان در مقابل این سئوال که به‌طورکلی آیا این ستاد می‌تواند جای خالی فعالیت خاصی را پر کند،

مردد هستند و پاسخ‌های بله و خیر به‌هم نزدیک است.

اما در مقابل، تعداد نهادهای ناظر در موضوع امنیت فضای سایبری را زیاد ارزیابی می‌کنند.



در ادامه از تعداد نهادها، پرسیده شد که آیا این نهادها با یکدیگر تداخل وظایف دارند که اکثریت قاطع معتقد به تداخل وظایف هستند و آن را ناشی غیردقیق بودن مأموریت می‌دانند. سایر مواردی که به آن اشاره شده بود یعنی ذات نادقیق فعالیت‌ها، تعریف مناسب وظایف و ناکافی بودن تعداد نهادها، آرای کمی را جلب کردند.



بخشی از نظرسنجی نیز به درج نظرات و توضیحات پاسخ دهندگان اختصاص داشت.

دیدگاه‌های بسیار جذابی در بین این نظرات دیده می‌شود که نشان می‌دهد اگر در تدوین اساسنامه ستاد، از دیدگاه‌های گوناگون استفاده شود تا چه حد می‌تواند به غنای آن بیفزاید. در ادامه برخی از این دیدگاه‌ها را می‌خوانید.

برخی نظرات مقداری جرح و تعدیل شده‌اند.

در مورد تداخل وظایف نهادهای ناظر نوشتند ... (۱)

مدیر ارشد: فضای امنیت سایبری کشور نظام‌مند و یا سیستماتیک نمی‌باشد. از طرف دیگر شاید تخصص‌ها نیز در حد قابل قبول و قابل اتکایی نیست.

مدیر ارشد: پدافند غیرعامل: ادعا بالا و تخصص پایین. کلا نیرو ندارند. فقط بخشنامه ابلاغ می‌کنند. پلیس فتا: تو بحثای فنی و سرویس‌های تخصصی سازمان ضعیف.یک برگه میارن میگن امضا کنین اگر هک شدین باهاتون برخورد می‌کنیم. مرکز افتا: از پدافند و فتا بهترن بالاخره چهار تا نیرو دارن اما همون‌ها هم بعد مدتی از افتا میرن و جذب شرکت‌ها می‌شن. ICT: کلا طرف سازمان‌ها پیدا نمیشن. اصلا نیرو ندارن. بیان هم کسی به حرفشون گوش نمیکنه.

مدیر بخش خصوصی: امنیت سایبری نیاز به یک مدیریت واحد دارد که از مجرای آن دستورالعمل ها و الزامات امنیتی به دستگاه ها و بخش خصوصی ابلاغ شود. هر نهاد ناظر می‌خواهد که برای فعالیت در دستگاه از آن نهاد مجوز فعالیت اخذ کنیم. به عنوان بخش خصوصی وقتی وارد یک سازمان می‌شویم با طیف وسیعی از طرح‌ها و الزامات امنیتی مواجه می‌شویم که بخش زیادی از آنها با هم همپوشانی دارند. این موضوع سبب شده مدیر دستگاه نداند که برای اجرای کدام طرح امن‌سازی از ظرفیت بخش خصوصی استفاده کند. سندی است با نام نظام ملی پیشگیری که در آن سند به ظاهر تقسیم کار شده است اما در جلسات با سازمان ها مشاهده می‌شود که سایر دستگاه‌ها نیز اقدام به ابلاغ دستورالعمل‌های امنیتی می‌نمایند. به عنوان تجربه مکرر اینجانب و تیم تخصصی همراه در شرکت، اعلام می‌داریم که این شکل از موازی کاری نه تنها در ارتقاء امنیت سایبری کشور تاثیر چندانی نخواهد داشت بلکه بسیاری از اقدامات دارای اولویت را با تاخیر در اجرا مواجه خواهد کرد.

در مورد تداخل وظایف نهادهای ناظر نوشتند ... (۲)

مدیر میانی دولتی: الف – موازی کاری‌های متعدد و شفاف نبودن وظایف هریک. ب – مشخص نبودن یک نهاد بالادستی که مابقی نهادها از آن حرف شنوی داشته و آن نهاد حکم مرجع را داشته باشد. پ – غیرکارشناسی بودن و غیرمتخصص بودن تیم‌ها. ت – ایجاد سردرگمی برای کاربران و کارکنان دستگاه‌های گوناگون که هریک به نوعی زیر نظر بخش‌های داخلی مشغول به فعالیت می‌باشند.

مدیر ارشد خصوصی: پدافند غیرعامل و افتا تداخل وطیفه دارند و شرکت‌ها موظف هستند مجوز هر دو را دارا باشند که امری غیرضروری و زمان‌بر است.

مدیر ارشد: ارائه چندین مجوز از جهت کار در بخش دولتي باعث رانت مي‌شود و همه شرکت‌ها قادر به تامین همه مجوزها نیستند.

کارشناس بخش خصوصی: پدافند غیرعامل و افتای حوزه سابیری بهتر است به طور کامل به افتا واگذار شود.

مدیرمیانی بخش نیمه دولتی: پرسنل فعال در افتا بالاخص در شهرستان‌ها، شرح وظایف مشخصی ندارند و چون کم سابقه هستند، هیچ‌یک از جلسات به نتیجه درستی نمی‌رسد. کارهایی که به افتا ختم می‌شود پایان مشخصی ندارد و منتظر ماندن برای اعلام نظر افتا قاعدتا به کنسل‌شدن مناقصات و ایجاد ابهام در پروژه ها می‌انجامد.

مدیرمیانی بخش نیمه دولتی: ما در حوزه صنعت و انرژی هستیم. دستورالعمل از افتا، پدافند، حراست کل، حفاظت‌های صندوق‌ها، هلدینگ‌ها و ...

در مورد تداخل وظایف نهادهای ناظر نوشتند ... (۳)

کارشناس خانم از بخش نیمه دولتی: همه نهادها فقط به ارسال نامه می‌پردازند و کمک زیادی جهت رفع مشکلات انجام نمی‌دهند.

مدیر ارشد: هیچگونه شرح وظایف دقیقی از سازمان‌ها منتشر نشده است و این باعث دوباره کاری می‌گردد. برخی اوقات شرح وظایف آزمایشگاه‌ها را مجددا مدیریت راهبردی افتا مطالبه می‌کند. نبود نهاد نظارتی بر عملکرد نهادهای امنیت فضای سایبری.

مدیرمیانی دولتی: این چند سازمان کارهای مشابه هم انجام می‌دهند و کارهای انجام شده بدون نظارت دقیق و بدون بودجه و زیرساخت مناسب انجام می‌شود.

مدیر میانی: معمولا بدون در نظر گرفتن شرایط کسب‌وکارها و حتی سازمان‌ها و نظرخواهی از کارشناسان ... پشت درهای بسته و با نگاه صرفا امنیتی تصمیماتی می‌گیرند که منجر به توزیع رانت می‌شود و ابلاغیه‌ها .. با این هدف انجام می‌شود که بعد از یک رخداد سایبری بتوانند از خود رفع مسئولیت کنند.

مدیر ارشد: ۱-نبودن نظام استاندارد، ۲- نبود زیست چرخ مدیریت امنیت در کشور، ۳- عدم تعیین دقیق تضاد منافع در نظام مدیریت امنیت کشور، ۴-نبود نظام‌نامه ثابت دقیق و جامع، ۵-عدم تربیت نیروی انسانی متناسب، ۶- نبود ساختار شغلی متناسب با مسئولیت مدیریت امنیت، و چندین و چند موضوع با اهمیت مانند امنیتی سازی موضوع مدیریت امنیت فناوری اطلاعات.

مدیر ارشد: اساسا" متولی امنیت باید خود سازمان بهره بردار باشد. اینکه یک سازمان سومی مثل مرکز افتا یا پدافند غیرعامل بیاید و به بهره بردار تاییدیه بدهد تضمین کننده امنیت نیست! امنیت تیم عملیاتی داخلی می‌خواهد، امنیت فرهنگ سازی و آموزش می‌خواهد، امنیت مراقبت لحظه‌ای میخواهد و ...

برخی نظرات مقداری جرح و تعدیل شده‌اند.

در مورد تداخل وظایف نهادهای ناظر نوشتند ... (۴)

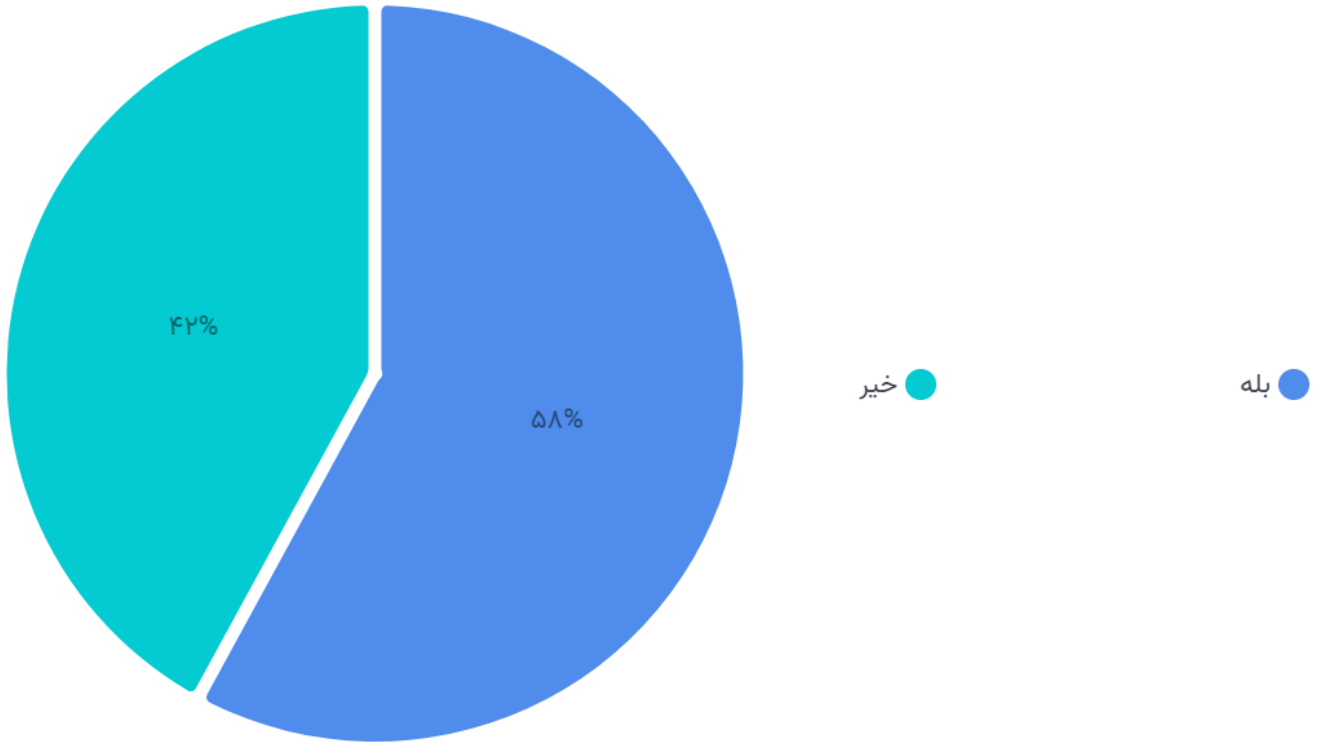
مدیر ارشد خصوصی: ضرورت دارد نهاد سیاست‌گذار، نهاد قانون‌گذار، نهاد(های) مجری، نهاد ناظر و نهاد رسیدگی به شکایات، با تفکیک شفاف و با شرح وظایف و مرز اختیارات مشخص وجود داشته باشد که اینطور نیست.

مدیر ارشد: ستاد باید فقط فعالیت ستادی داشته باشد، دولت باید حمایت، هدایت و نظارت داشته باشد و این ستاد ماموریت را به درستی انجام دهد و به هیچ وجه وارد اجرا نشود.

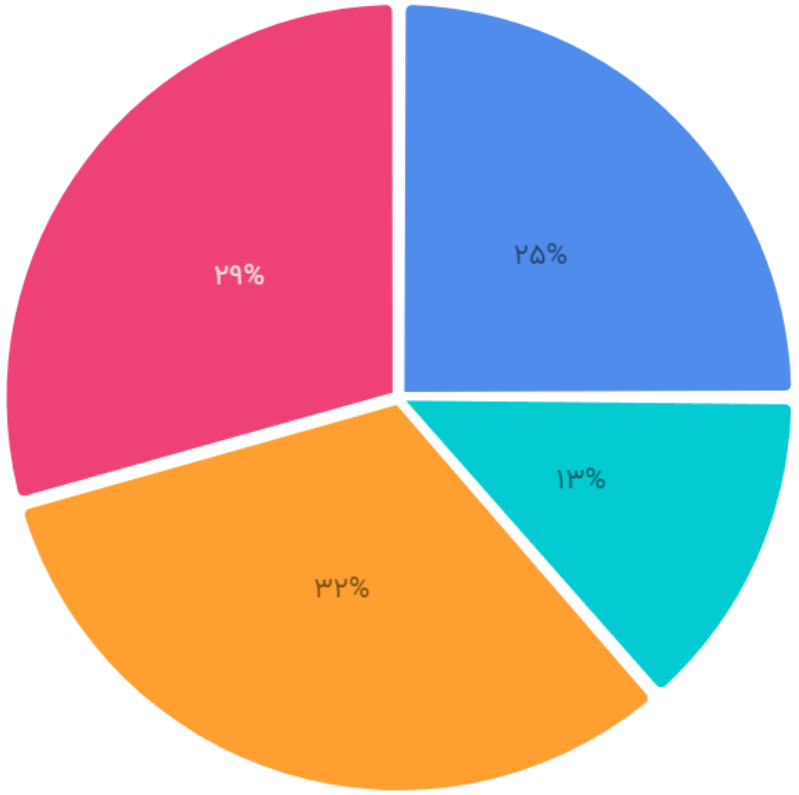
مدیر میانی: اساسا نهادهای ناظر می‌بایست وظایف رگولاتوری و وضع استانداردها را برعهده بگیرند و پیاده سازی بر عهده سازمان‌ها باشد. در حالیکه الان در ریزترین مسائل دخالت می‌کنند و کوچک‌ترین چیزی را هم گردن نمی‌گیرند.

مدیر ارشد دولتی:اصولا موضوع دفاع لایه به لایه به‌معنای ساختن مکانیزم های دفاعی در سطح زیرساخت و نیروی انسانی در سازمان‌ها می‌باشد. تفکیک سازمان‌ها به حیاتی و غیرحیاتی وقتی بسیاری از چالش‌های سایبری از ارتباطات این سازمان ها منبعث می‌شود و اینکه افتا در تعامل جدی با حراست سازمان ها بوده ولی وزارت ICT دسترسی به این حوزه ندارد قطعا تاثیر گذار خواهد بود.

درمورد خالی بودن جای یک نهاد فرضی نیز اجماعی وجود ندارد و نظرات موافق و مخالف نزدیک است.



سئوال مهم بعدی درباره فلسفه تشکیل این نهاد از دیدگاه پاسخ دهندگان بود. اینکه چقدر تشکیل این نهاد در راستای برنامه‌های کلی دولت ارزیابی می‌شود یا تقویت بخش خصوصی. در اینجا پراکندگی دیده می‌شود. تقریبا یک سوم به اساسنامه این ستاد چشم دوخته‌اند و یک سوم نیز تقویت بخش خصوصی را در دستور کار نمی‌بینند که این زنگ خطر مهمی را به‌صدا در می‌آورد.



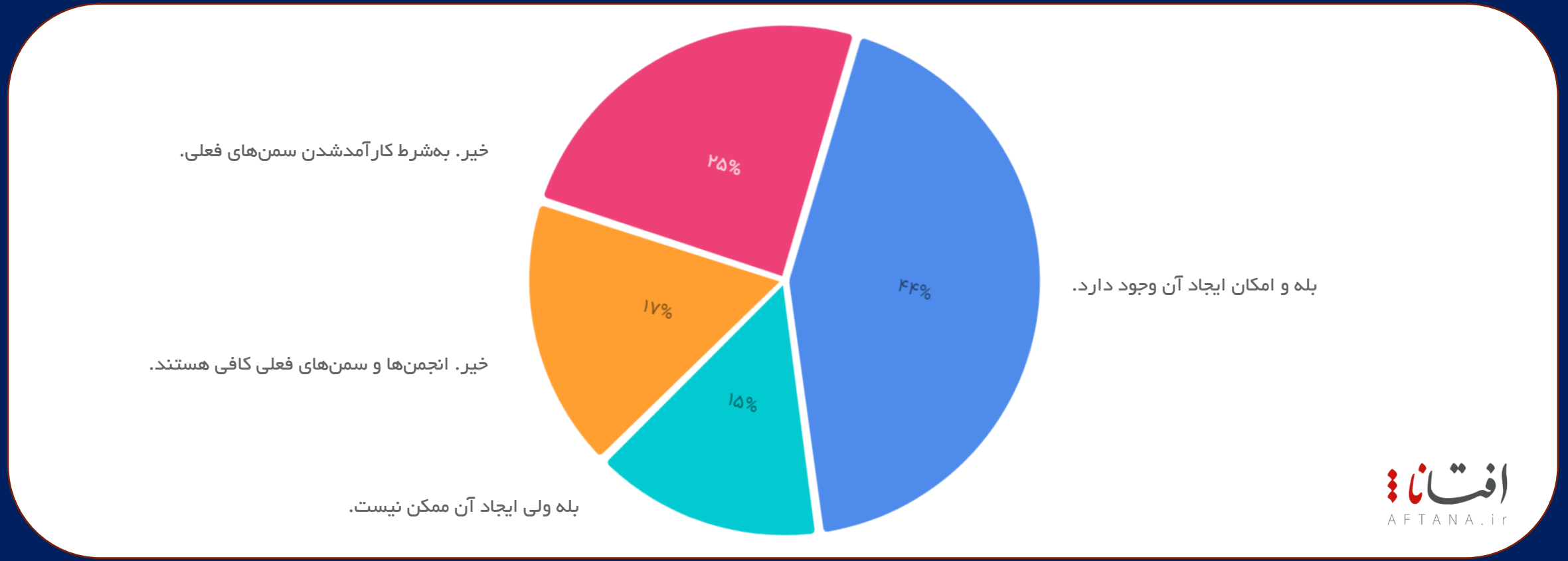
تقویت نظارت حاکمیتی

تقویت نظارت حاکمیت و رونق بازار بخش خصوصی

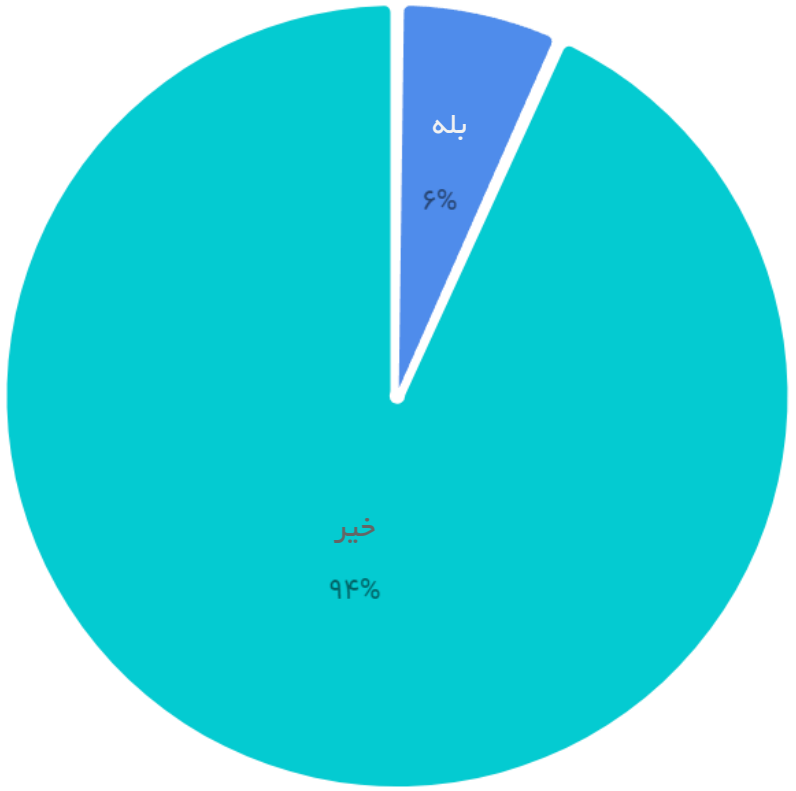
بستگی به اساسنامه آن دارد و ممکن است هرکدام از موارد فوق باشد

اساساً تقویت بخش خصوصی در دستور کار نیست

سئوال بعدی به جایگاه بخش خصوصی در این زمینه معطوف بود. اینکه در این موضوع، آیا جای نهاد مستقل نظارتی بخش خصوصی خالی است یا خیر. نزدیک به نیمی از پاسخ‌ها مثبت است. یک چهارم معتقدند که نهادهای موجود بخش خصوصی باید توانمند شوند و نیازی به نهاد جدید نیست. ۱۷درصد نیز همین نهادهای فعلی را کافی می‌دانند و ۱۵درصد نیز معتقدند که علیرغم نیاز به چنین نهادی؛ امکان تشکیل آن وجود ندارد.



سئوال آخر نیز نشان می‌داد که از بین پاسخ دهندگان تنها تعداد بسیار اندکی برای تهیه پیش‌نویس و اساسنامه ستاد مورد مشورت قرار گرفته‌اند.



در انتها نیز از پرسش‌شوندگان درخواست شد که نظرات تکمیلی خود را درج کنند.

این بخش نیز حاوی نظرات جذابی است که بعضی از آن‌ها را می‌خوانید.

برخی نظرات مقداری جرح و تعدیل شده‌اند.

به‌عنوان نظرات و دیدگاه‌های تکمیلی نوشتند ... (۱)

مدیر ارشد: نظارت امنیت سایبری باید دست یک سازمان و زیرنظر دولت باشد. نظامی‌ها نباید به زیرساخت بخش دولتی نظارت کنند چون شناخت کمی از این حوزه دارند و باید حوزه نظامی سایبری کشور را قوی کنند.

مدیر ارشد: بخش خصوصی باید در تدوین اساسنامه ها، طرح های امن سازی، الزامات امنیتی و سایر تصمیمات این حوزه نقش فعالی داشته باشد. به دفعات مشاهده شده که دستورالعملی ابلاغ شده و قابلیت اجرا نداشته است و این موضوع مشکلات فراوانی را برای دستگاه و شرکت به وجود آورده است.

مدیر ارشد خصوصی: گسترش بوروکراسی و افزودن دفتر و دیوان سازمان تازه به مساله نه تنها دردی را دوا نمی‌کند که ریشه بسیاری از گرفتاری‌های کشور است. درمان درد این کشور در هرس‌کردن شاخ و بال بوروکراسی است.

مدیر میانی دولتی: به نظر می رسد این نهادها از سازمان ها و وزارتخانه‌های خاصی تبعیت می‌کنند و بیشتر نقش ایشان سیاسی است تا تخصصی و کاربردی.

مدیر میانی دولتی: در بسیاری از ادارات و نهادهای دولتی افرادی هستند که کاملا به امور سایبری مسلط می باشند اما از آنها در این امور استفاده نمی‌شود و یا حتی فراخوانی جهت دعوت از ایشان صورت نگرفته است.

به‌عنوان نظرات و دیدگاه‌های تکمیلی نوشتند ... (۲)

مدیر میانی نیمه‌دولتی: خیلی شفاف عرض می‌کنم که ما در ایران مدیر کم نداریم و همه شغل نظارت دارند و این ضربه بزرگی به بدنه امنیت خواهد زد. ما نیاز به افراد، انجمن‌ها و نهادهای اجرایی داریم که کارشان حذف صورت مسئله و پاک کردن اصل موضوع به دلیل دانش اندک نباشد بلکه افرادی باتجربه باشند که در راستای ایجاد بنیه امنیتی به همگان کمک کنند و ایجاد سد ننمایند.

کارشناس خصوصی: یکی از دلایل ناکارآمدی این ارگان ها، نبود هدف درست و شرح وظایف می‌باشد. همچنین اعمال محدودیت‌هایی از جمله الزام به تهیه محصولاتی که خود ساده‌ترین تست‌های آزمایشگاهی را نمی‌توانند پاس کنند.

مدیر ارشد بخش خصوصی: شایسته است این نهاد از طرف بخش خصوصی وظیفه هماهنگی و نظارت بر عملکرد کند و کسل کننده نهادهای مربوطه را برعهده بگیرد.

مدیر میانی بخش دولتی: اجرا و نظارت دقیق و ایجاد بستر و امکانات مناسب در تمام ارگان‌های دولتی و خصوصی مرتبط با موضوع لازم و ضروری می‌باشد. درغیر این صورت اضافه کردن نهادهای بیشتر فقط هزینه‌های دولت را بیشتر می‌کند.

مدیر میانی بخش خصوصی: به‌نظر من اصلی‌ترین کمبود، نبود هیچ گونه سامانه‌ای برای به اشتراک‌گذاری رخدادها است.نیاز است پلتفرمی ایجاد شود برای اطلاع رسانی حملات درحال انجام در کشور و همچنین به تفکیک صنایع مختلف و اشتراک گذاری نتایج فارنزیک. همچنین جای خالی انجمن های تخصصی برای هم افزایی و انتقال تجربیات در بخش خصوصی به‌شدت محسوس است.

به‌عنوان نظرات و دیدگاه‌های تکمیلی نوشتند ... (۳)

کارشناس بخش خصوصی: بیشتر نیاز به نظارت بر خود دستگاه ها احساس می‌شود، در صورت قصور و کوتاهی هر ارگانی؛ هیچ جایی مطالبه نمی‌کند و اگر هم مطالبه کند پاسخ مناسبی دریافت نمی‌شود. هر ارگان و دستگاهی می‌بایست نسبت به اشتباهات و کوتاهی‌ها پاسخگو باشد و نهادهای زیربط بایستی تا دریافت گزارش کامل پیگیر موضوعات باشند ، در انتها موارد قابل ارائه در اختیار عموم قرار گیرد.

مدیر ارشد بخش خصوصی: به‌نظر بنده این ستاد باید با هماهنگی و اخذ نظرات همه نهادهای ذیربط و کل بازیگران اکوسیستم امنیت سایبری کشور، دستورالعمل‌ها و نظام‌نامه‌های جدید، جامع و شفافی تهیه کند و ضمن ابلاغ آنها به کل اکوسیستم، کلیه ابلاغیه‌های قبلی همه نهادهای امنیتی سایبری را یک‌جا باطل نماید.

مدیر ارشد بخش خصوصی: در این نظر سنجی موارد دیگری هم می‌شد پرسید. مثلا: ذینفعان این ساختار چه کسانی باید باشند، زیست چرخ این ساختار بر اساس چه مدل استاندارد تهیه شده و اساسا زیست چرخی دارد یا نه، ابزارهای مدیریتی و کنترلی این ساختار در کشور چه خواهد بود، اساسا این ساختار با این همه ساختار دیگر چگونه ارتباط برقرار خواهد کرد.


افتا
AFTANA.ir
نخستین پایگاه خبری امنیت سایبری کشور