چالش‌های آگاهی رسانی امنیتی سازمانی

بزرگ‌ترین چالش

یکی از موضوعات کلیدی که نیازمند درک آن هستیم، آگاهی از چالش‌های اساسی آگاهی رسانی امنیتی (Security Awarness)، مشکلاتی که با آن مواجه هستند و طریقه کمک ما به‌عنوان یک اجتماع به آنهاست. پس ما این سوال را مطرح می‌کنیم: بزرگ‌ترین چالش شما چیست؟ همان گونه که در شکل زیر مشخص است، ما در این باره بیش از صد ها پاسخ مختلف دریافت کرده‌ایم.

سر در گم شدید؟ بله، ما نیز همین طور بودیم. خوش‌بختانه اینگولف بکر از دانشگاه لندن، این پاسخ‌ها را در ۱۲ گروه مختلف، همان گونه که در جدول زیر مشاهده می‌کنید جای داده‌است. ۷ قسمت اول شامل ۹۳ درصد از پاسخ‌هاست که ما بر روی آنها متمرکز می‌شویم.

جدول‌بندی بزرگ‌ترین چالش‌هایی که برنامه‌های آگاهی‌بخشی امنیت با آن مواجه‌اند:

نوع مشکل	تعداد پاسخ	درصد
منابع	۵۰	۱۹
اتخاذ تصمیم	۴۸	۱۹
پشتیبانی از سوی مدیریت	۴۷	۱۸
پشتیبانی کاربر	۲۷	۱۰
پیدا کردن زمان برای مشارکت	۲۴	۹
محتوا	۲۳	۹
کمبود آگاهی پرسنل	۲۲	۹
اجباری نبودن	۹	۳
مشکلات دپارتمان حقوقی	۴	۲
بدون مجازات بودن	۲	۱
ترجمه متون	۱	۰/۵
معیارهای مبهم	۱	۰/۵

اولین موضوعی که به چشم می‌آید این است که ۷ گروه اول، خود در داخل ۲ گروه عمومی قرار می گیرند: کمبود منابع، پشتیبانی و زمان و یا نداشتن تاثیر. افراد یا در توانایی خود برای اجرا کوتاهی کرده و یا نمی‌توانند تاثیر لازم را داشته‌باشند. این موضوع معمای «داستان دو چالش» است. سایر قسمت‌های این گزارش شامل مشخص کردن و فهم این چالش‌ها و شناسایی راه‌حل‌های موجود است.

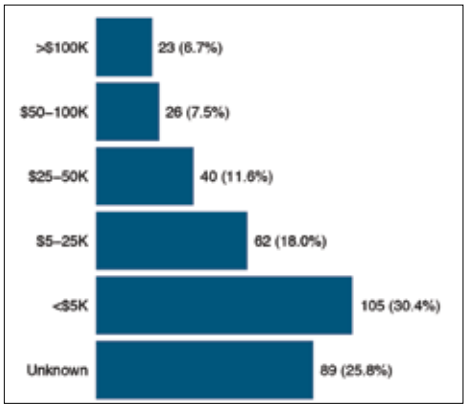
منابع، پشتیبانی و زمان (و یا کمبود آنها)

این موضوع برای کسانی که گزارش سال گذشته را مطالعه کرده‌اند، مایه حیرت نخواهدبود. داده‌ها نشان می‌دهند که بسیاری از کارکنان آگاهی‌رسانی امنیتی از کمبود منابع، پشتیبانی و زمان برای انجام وظیفه‌شان رنج می‌برند. به‌طور کلی وضعیت نسبت به سال گذشته بهبود یافته است، اما نه به اندازه کافی. اینگلف این سه دسته را این گونه تعریف می‌کند:

- **منابع:** کمبود منابع فنی و مالی
- **پشتیبانی مدیریت:** مافوق‌ها ضرورت کمپین‌های آگاهی‌رسانی امنیتی را نمی‌بینند و یا با آنها همکاری نکرده و برای تسهیل این امر عملی انجام نمی‌دهند.
- **کمبود نیروی کار آگاهی‌رسانی امنیتی:** این امر نیازی به توضیح ندارد.

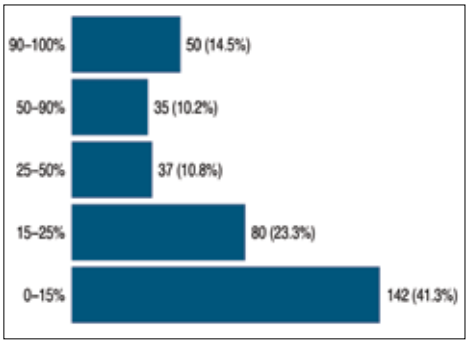
در زمینه بودجه باید گفت که بیش از ۵۰درصد گزارش‌ها حاکی از آن است که کارکنان آگاهی‌رسانی امنیتی، بودجه‌ای کمتر از ۵۰۰۰ دلار داشته و یا از داشتن بودجه بی‌خبرند. تنها ۲۵ درصد از گزارش‌ها دارای بودجه‌ای بالغ بر ۲۵ هزار دلار هستند. قطعا انتظار می‌رود که بودجه‌های بیشتر مخصوص شرکت‌ها و مؤسسات بزرگ‌تر باشند، اما مشاهده می‌شود که مؤسسات بزرگ و کوچک هر دو دارای چنین بودجه‌هایی هستند.

بودجه تخمینی سال ۲۰۱۶



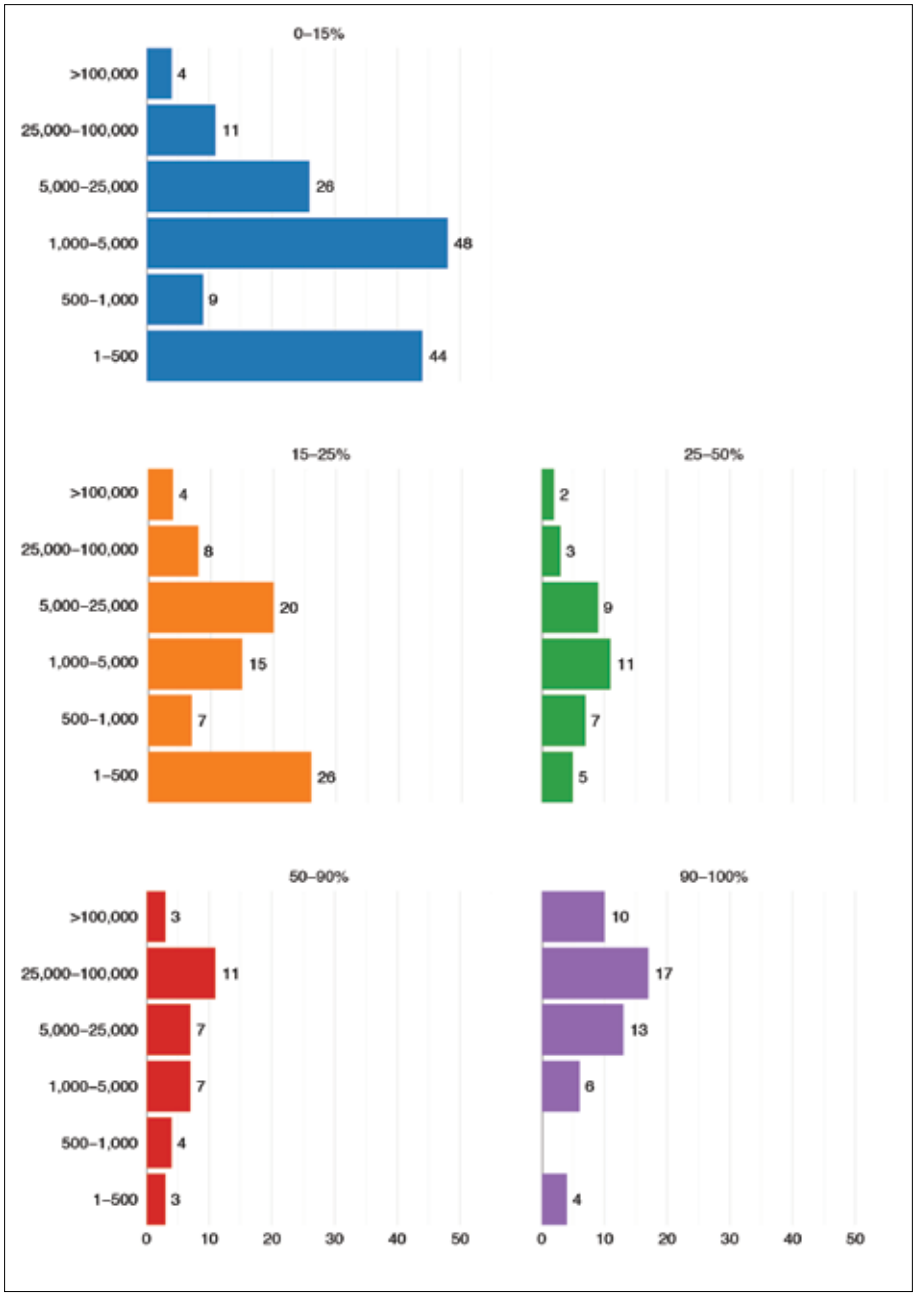
به علاوه، افراد چقدر زمان صرف پرداختن به آگاهی‌رسانی امنیتی خود می‌کنند؟ اکثر اوقات مشاهده می‌شود که پرداختن به مقوله آگاهی یکی از بی‌شمار وظایفی است که افراد دارا هستند. کمتر از ۱۵ درصد افراد به‌طور تمام‌وقت روی مقوله آگاهی کار می‌کنند. با اینکه این امر بهتر از آمار ۱۰ درصدی سال گذشته‌است، مشاهده می‌شود که بیش از ۶۵ درصد افراد کمتر از یک‌چهارم زمان خود را صرف این مقوله می‌کنند. اکثر افراد در بهترین شرایط، ۱۰ ساعت در هفته روی مقوله امنیت فعالیت می‌کنند. تصور کنید که امنیت مؤسسه و شرکت شما چگونه خواهدبود اگر تیم‌های پاسخ به حادثه و امنیت شبکه‌تان کمتر از ۱۰ ساعت در هفته برای انجام مسئولیت‌شان وقت بگذارند.

زمانی که صرف آگاهی‌رسانی امنیتی می‌شود



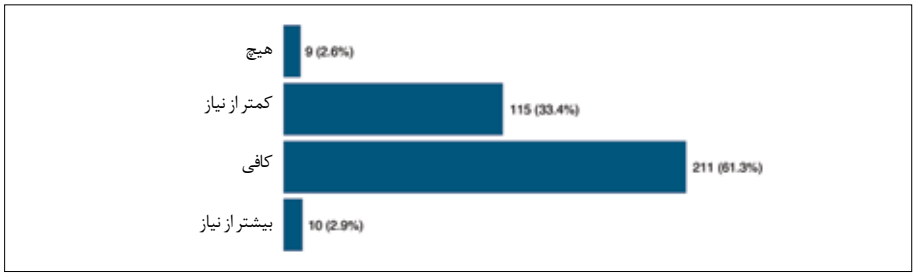
این مشکل تنها مختص مؤسسات و شرکت‌های کوچک نیست. شمار کسانی که به‌صورت نیمه‌وقت روی مقوله آگاهی فعالیت می‌کنند در تمامی مؤسسات، چه کوچک و چه بزرگ در حال افزایش است. این امر به این معنی است که تمامی تلاش‌ها در این زمینه به‌صورت نیمه‌وقت بوده و به‌علاوه می‌توان گفت که برای تعداد زیادی از اشخاص، آگاهی مقوله‌ای است که باید علاوه‌بر شغل اصلی‌شان به آن بپردازند و به‌صورت کامل روی آن تمرکز ندارند.

زمان صرف‌شده بر روی آگاهی‌رسانی امنیتی بر حسب اندازه شرکت



درنهایت، آیا برنامه‌های آگاهی‌رسانی امنیتی، پشتیبانی اجرایی مورد نیاز را دارند؟ موضوع دلگرم‌کننده این است که بیش از ۶۰ درصد افراد گزارش داده‌اند که پشتیبانی موردنظر را دارند. با این وجود هنوز ۳۵ درصد دارای پشتیبانی لازم برای موفقیت نیستند.

میزان پشتیبانی اجرایی

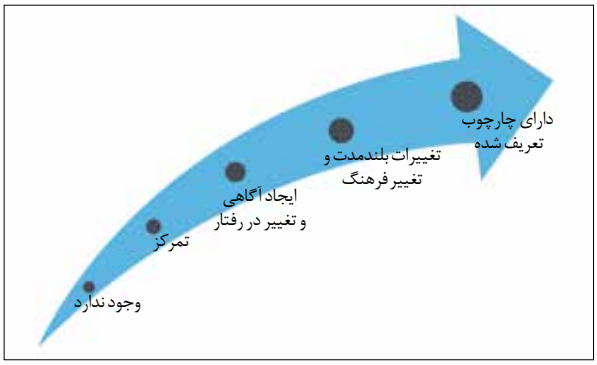


داده‌ها نشان می‌دهد که از میان سه عاملی که اینگلف آنها را مشخص کرده‌است (منابع، زمان/نیروی کاری و پشتیبانی اجرایی)، پشتیبانی بیشترین تاثیر را بر موفقیت این امر داشته‌است. تحقیقاتی که توسط گریس رچمر انجام شده ارتباط قدرتمندی را بین این دو مقوله نشان می دهد. بنا به این گزارش‌ها هرچه پشتیبانی اجرایی و آگاهی افراد بیشتر باشد، برنامه آگاهی‌رسانی امنیتیی بلوغ بیشتری خواهند داشت. میزان بالغ بودن صنعت آگاهی‌رسانی امنیتی توسط مدل بلوغ آگاهی‌رسانی امنیتی مشخص می‌شود.

این مدل که در سال ۲۰۱۱ ایجاد شده‌است، باعث شد تا مؤسسات و شرکت‌ها بتوانند میزان پیشرفت برنامه آگاهی‌رسانی امنیتی خود، میزان پیشرفت آن در صورت وجود یک مدیر شایسته و راه رسیدن به آن را بدانند. این مدل بر اساس پنج مرحله مختلف طراحی شده که هر قسمت بر پایه قسمت قبلی است.

مدل بلوغ آگاهی‌رسانی امنیتی

- **معدوم:** برنامه آگاهی‌رسانی امنیتی وجود ندارد. کارکنان هیچ اطلاعاتی در رابطه با اینکه هدف حملات امنیتی بوده، اعمال‌شان اثر مستقیم بر امنیت شرکت داشته، سیاست‌های شرکت چه بوده و چطور به آسانی می‌توانند طعمه حملات امنیتی قرار بگیرند، ندارد.
- **بر طبق دستور:** برنامه آگاهی‌رسانی امنیتی در وهله اول برای پیروی از دستورات و قوانین خاص یا برای بازرسی‌ها طراحی شده‌است. آموزش‌ها محدود و به‌صورت سالیانه و یا تنها برای یک منظورهستند. کارکنان از سیاست‌های شرکت یا از نقش خود در راستای محافظت از دارایی‌های اطلاعاتی شرکت، اطمینان ندارند.
- **آگاهی ترقی یافته و تغییر در رفتار:** برنامه آگاهی‌رسانی امنیتیی، موضوعاتی که بیشترین تاثیر را در پشتیبانی از هدف شرکت دارند شناسایی کرده و تمرکز خود را بر روی آنها می‌گذارد. برنامه پارا از آموزش‌های سالیانه فراتر گذاشته و در طی سال به‌صورت مستمر تقویت می‌شود. محتوای این برنامه‌ها طوری منتقل می‌شوند که باعث تغییر رفتار در محل کار، خانه و هنگام مسافرت، می‌شود؛ درنتیجه افراد از سیاست‌های شرکت در این زمینه پیروی کرده و فعالانه حوادث را شناخته از وقوع آن جلوگیری کرده و آنها را گزارش می‌کند.
- **پایداری طولانی‌مدت و فرهنگ‌سازی:** برنامه آگاهی‌رسانی امنیتیی دارای فعالیت‌ها، منابع و پشتیبانی مدیریت برای داشتن چرخه عمر بالا است. این امر شامل حداقل یک بررسی و یک به‌روزرسانی به‌صورت سالانه است؛ درنتیجه این برنامه به‌عنوان قسمتی از فرهنگ شرکت در جریان و قابل توجه است.
- **چارچوبی برای اندازه‌گیری:** برنامه آگاهی دارای یک چارچوب قدرتمند برای اندازه‌گیری و بررسی پیشرفت و میزان تاثیر است؛ درنتیجه این برنامه به‌طور مداوم بهبود یافته و هزینه‌های صرف‌شده بر روی آن را برمی‌گرداند. این مرحله بدین معنی نیست که سایر مراحل این چارچوب را ندارند بلکه این نکته را خاطرنشان می‌کند که برای داشتن یک برنامه آگاهی‌رسانی امنیتیی بالغ و رسیدن به موفقیت، شما باید این چارچوب را داشته‌باشید.



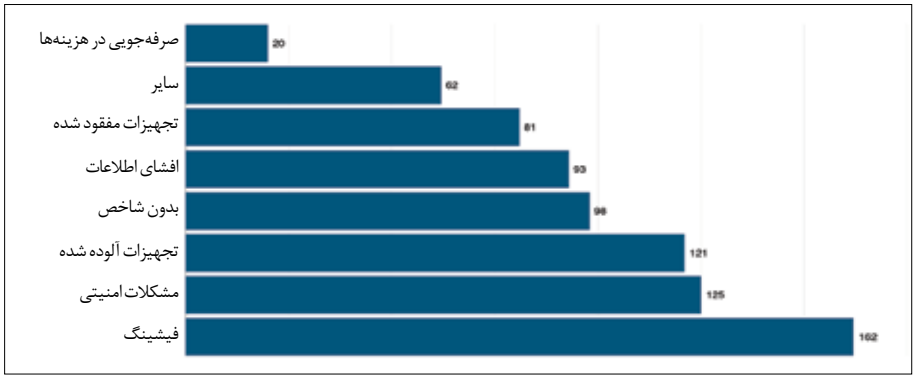
گریس به این نکته پی برد که برنامه‌هایی که میزان بلوغ آن‌ها در مرحله معدوم است ارتباط مستقیمی با پشتیبانی اجرایی دارند. در مقابل، بالغ‌ترین مراحل (فرهنگ‌سازی و چارچوب اندازه‌گیری) محال است بدون این پشتیبانی باشند. همان‌طور که در نمودار زیر مشخص است، پشتیبانی اجرایی بیشترین تاثیر را بر میزان بلوغ یک برنامه آگاهی‌رسانی امنیتی دارد.

نمودار بلوغ در برابر پشتیبانی اجرایی

درنهایت، ما این سوال را پرسیدیم که شرکت‌ها و مؤسسات، چگونه میزان آگاهی خود را از مسائل امنیتی می‌سنجند. ما اعتقاد داریم که یکی از دلایل کلیدی که باعث می‌شود برنامه‌های آگاهی دارای پشتیبانی مدیریت نباشند وجود تعداد بسیار کمی از اندازه‌گیری‌هایی است که مشکلات انسانی و تاثیر برنامه آگاهی بر حل این مشکلات را مشخص می‌کنند. پدیده فیشینگ (فرستادن ایمیلی به‌عنوان شرکت‌های معتبر توسط هکرها برای به‌دست آوردن اطلاعات شخصی) یکی از بهترین معیارها

در این زمینه اســـت. این پدیده نه‌تنها یک خطر جدی انســـانی به حســـاب می‌آید بلکه یک روش موثر برای اندازه‌گیری خطر است. با این حال، پدیده فیشینگ یکی از خطرات انسانی است که شرکت‌ها و مؤسسات با آن مواجه‌اند. لازم است که خطرات انسانی دیگر و ارزش برنامه آگاهی‌رسانی امنیتی را برای مؤسسات و شرکت‌ها، بهتر اندازه‌گیری کنیم.

معمول‌ترین معیارهای اندازه‌گیری



پیشنهادها

معمولا برنامه‌های آگاهی‌رسانی امنیتی بعدا به مؤسسات اضافه می‌شوند. بدین‌صورت که مسئولیت آگاهی به یک نفر به‌صورت تصادفی، بدون داشتن زمان، منابع و یا پشتیبانی مورد نیاز برای موفقیت، داده‌می‌شود. به‌علاوه آگاهی‌رسانی امنیتی معمولا در پاسخ به قوانین وضع شده ایجاد می‌شود تا یا در زمان بازرسی‌ها مورد استفاده قرار گیرد و یا افراد را با سیاست‌های شرکت در این زمینه آشنا سازد. ما برای این مشکل ۳ راه‌حل پیشنهاد می‌کنیم:

طرزفکر: افراد در صنعت ما از مدیریت تا درجات پایین‌تر، مقوله امنیت ســـایبری را صرفا جزء مشـــکلات فنی و مربوط به آی‌تی به حساب می‌آورند. باید سیستم مدیریت را به طرز بهتری آموزش دهیم تا درک کنند که امنیت سایبری یک مشکل انسانی نیز هست. تا زمانی که تنها روی راه‌حل‌های فنی در این زمینه سرمایه‌گذاری کنیم، بازنده نبرد امنیتی خواهیم‌بود.

مســـیر: معمولا سیســـتم مدیریت، خطرناک بودن رفتار افراد را برای مؤسسات درک می‌کند. مشکل اینجاست که سیستم مدیریتی آگاهی‌رســـانی امنیتی را راه‌حل مناســـبی در این مورد نمی‌داند. مســـئولان آگاهی‌رســـانی امنیتی باید این امر را خاطرنشان سازند که دارای مسیری مطمئن برای رسیدن به فرهنگ‌سازی برای امنیت هستند. مسیری که نه‌تنها بر اساس تئوری‌های آموزشی، مدل‌سازی رفتاری و مدیریت تغییر بوده، بلکه از تجارب دیگران نیز استفاده می‌کند.

معیارها: مشخص کردن تاثیر آگاهی‌رسانی امنیتی میسر نیست مگر با اندازه‌گیری خطرات انسانی و نشان دادن تاثیر شما بر روی آنها. این امر شروع تغییر برای جامعه‌ای است که هرروزه راه‌های جدیدی برای شناخت رفتارها و فرهنگ‌های امنیتی ابداع می‌کند. روش‌هایی که برای رسیدن به این مهم وجود دارند شامل ارزیابی دانش موجود در این زمینه، نظرسنجی‌ها و دیگر روش‌های ارزیابی رفتارها هســـتند. درنهایت ارزیابی‌های قدرتمندتری برای کمک به نشـــان دادن ارزش آگاهی‌رسانی امنیتی، نیاز است.

خوره‌های کامپیوتر آگاهی‌رسانی امنیتی را به ارث برده‌اند (آیا این خوب است؟)

در ادامه «داستان دو چالش» می‌بینیم که با اینکه اعضای تیم آگاهی‌رسانی امنیتی تمام منابع مورد نیازشان را دارا هستند، نمی‌توانند تاثیر دلخواهشـــان را داشته‌باشـــند. چرا این گونه اســـت و در این باره چه کاری می‌توان انجام داد؟ در ابتدا به سوال اصلی خود بازمی‌گردیم که «بزرگ‌ترین چالش شـــما چیســـت؟». اینگلف پاسخ‌هایی را که در ارتباط با نداشتن تاثیر به این

سوال داده شده‌است در چهار گروه دسته‌بندی کرد:

اتخاذ: کاربران نمی‌توانند رفتار خود را به‌وسیله آموزش تغییر دهند.

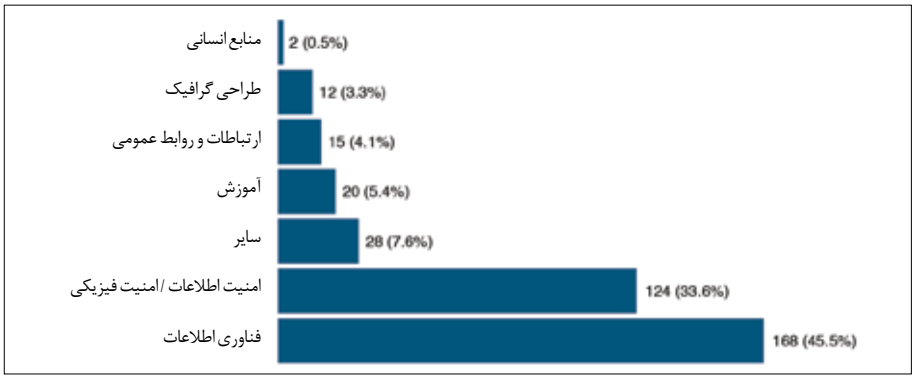
پشتیبانی کاربر: افرادی که باید در کمپین آگاهی‌رسانی امنیتی شرکت کنند، این کمپین را ضروری ندانسته و معمولا در آن شرکت نمی‌کنند.

پیدا کردن زمان: به‌دلیل کم‌اهمیت بودن این امر برای کاربران، آنها معمولا به‌سختی زمانی را برای مشارکت در این زمینه پیدا می‌کنند.

محتوا: مشارکت‌کنندگان در این زمینه معمولا به‌سختی می‌توانند محتوای مناسبی تهیه کنند.

ما کار خود را با ارزیابی مشارکت‌کنندگان در زمینه آگاهی‌رسانی امنیتی، شروع می‌کنیم. این‌طور که پیداست اکثریت افرادی که در آگاهی‌رسانی امنیتی مشارکت می‌کنند، خوره‌های کامپیوتر هستند. همان‌طور که در نمودار مشاهده می‌شود، ۷۹ درصد این افراد دارای پیش‌زمینه فنی هستند.

نقش‌های پیش از پیوستن به تیم آگاهی‌رسانی امنیتی



بخش بزرگی از هر برنامه آگاهی‌رسانی امنیتی به مهارت‌ها به‌خصوص در زمینه ارتباط بستگی دارد. برای متوجه شدن افراد، مشارکت‌کنندگان در مبحث آگاهی‌رسانی امنیتی باید برای آنها با زبانی ساده توضیح دهند که چرا آگاهی برای آنها اهمیت دارد و چه کاری باید انجام دهند. با این وجود اکثر افرادی که آگاهی‌های امنیتی را منتقل می‌کنند از کمترین مهارت ارتباطی ممکن برخوردارند. درواقع افراد دارای پیش‌زمینه‌های امنیتی، نامناسب‌ترین افراد برای انتقال آگاهی‌رسانی امنیتی هستند، چراکه دارای مشکلی به نام «نفرین دانش بیش از حد» هستند.

نفرین دانش بیش از حد، یک تعصب شناختی است. بدین معنی که هرچه شما در موضوعی خبره‌تر باشید، برایتان دشوارتر است تا آن موضوع را آموزش داده و منتقل کنید. متخصصان مبحث امنیت، این مبحث را به‌راحتی درک می‌کنند، چراکه به‌طور روزمره با آن سروکار دارند.

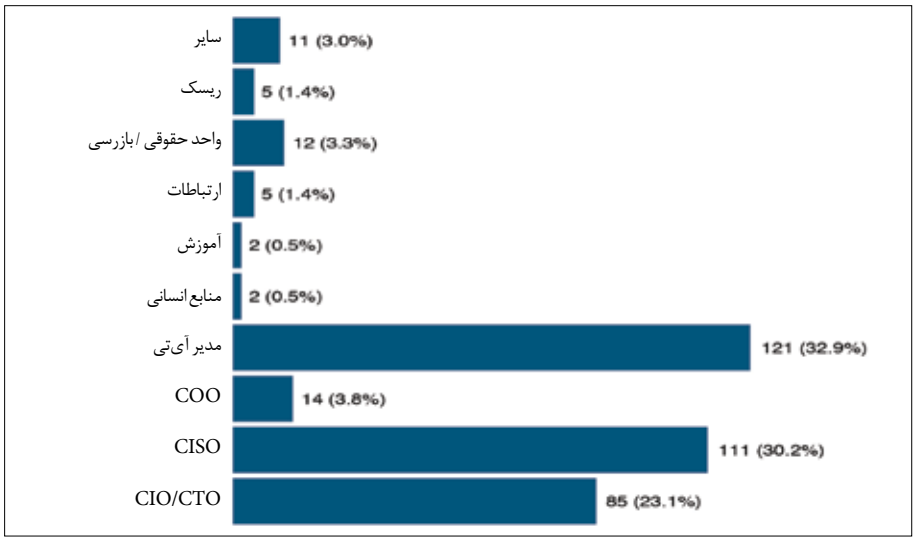
این افراد فرض می‌کنند که این مبحث برای سایر افراد شرکت نیز به همان سادگی است و برنامه آگاهی‌رسانی امنیتی خود را بر پایه این فرضیات بنا می‌کنند؛ درنتیجه اطلاعات نامناسبی را منتقل می‌کنند. بسیاری از افراد فنی از عدم درک این موضوع رنج می‌برند. یک مثال بارز این امر، کلمه عبور است. متخصصان امنیت همواره به افراد گوشزد می‌کنند که کلمات عبور پیچیده‌ای داشته‌باشند.

وقتی افراد از این امر سر باز می‌زنند، متخصصان گمان می‌کنند که این مشکل به دلیل عدم انگیزه است. پس وقت بسیاری را صرف توضیح دلیل اهمیت کلمه عبور پیچیده می‌کنند. در واقع، مشکل عدم انگیزه نیست، بلکه بسیاری از افراد کلمات عبور پیچیده را گیج‌کننده و دشوار می‌دانند.

به جای اینکه همواره به افراد گوشزد کنیم که این امر اهمیت دارد باید تمرکز خود را روی مقوله‌هایی مانند چگونگی ساده‌سازی کلمه عبور بگذاریم. برای مثال عبارات عبور را معرفی کرده، طریقه استفاده از نرم افزارهای مدیریت کلمه عبور را آموزش داده و یا به توضیح مبحث احراز هویت دو عاملی بپردازیم.

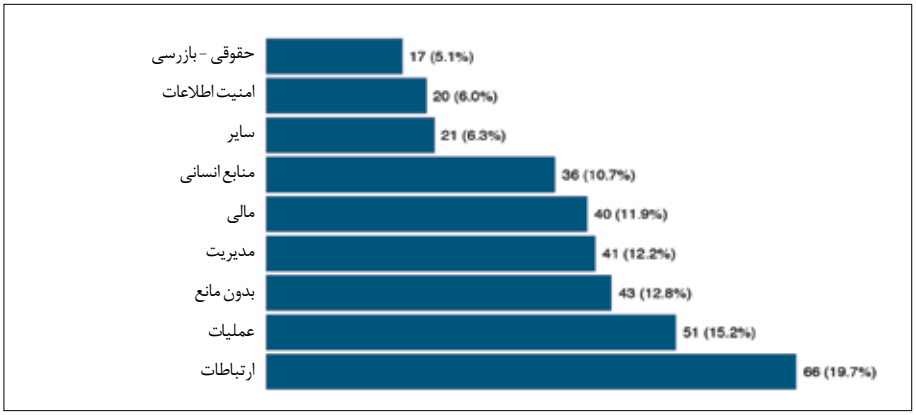
این امر نیز نگران کننده است که تنها ۴ درصد از مشارکت کنندگان در آگاهی‌رسانی امنیتی، دارای پیش‌زمینه ارتباطی هستند به‌خصوص در جاهایی که این امر حیاتی اســت. همان‌طور که در پایین مشــاهده می‌کنید، علاوه‌بر نامناسب بودن مهارت‌ها، بیش از ۹۰ درصد از برنامه‌های آگاهی‌رسانی امنیتی، وابسته به قسمت فنی هستند و به آنها گزارش می‌دهند.

محلی که به آن گزارش می‌شود



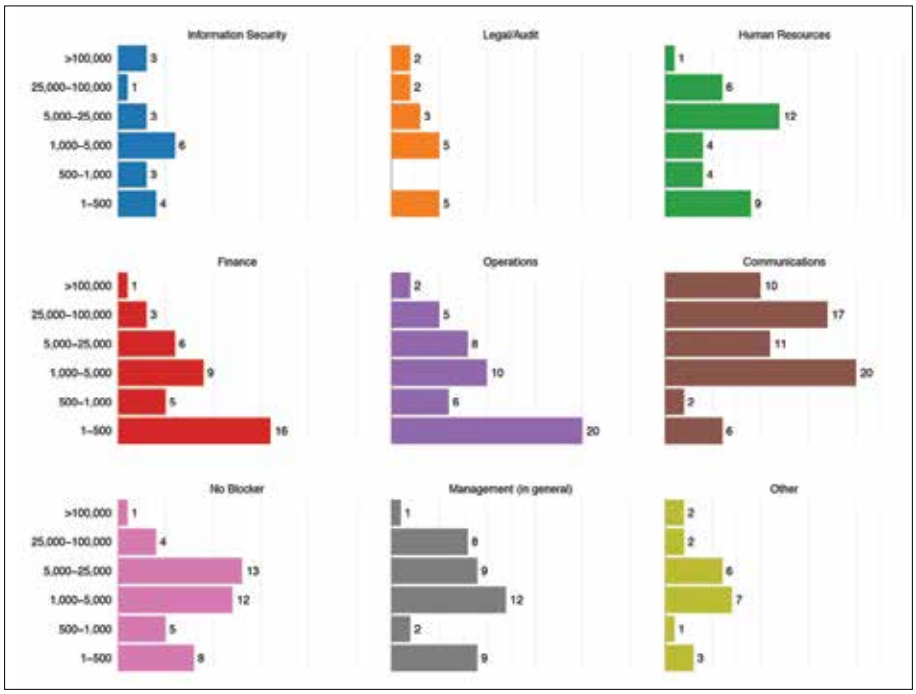
بزرگ‌ترین سد راه

آیا وجود آگاهی‌رســانی امنیتی در این قســمت لازم اســت؟ ما نمی‌دانیم. با این حال، اگر تیم آگاهی‌رسانی امنیتی شما در حوزه فنی قرار می‌گیرد، نیاز اســت تا روابط خوبی با قســمت ارتباطات شرکت داشته‌باشید. این امر، خود به این سوال منجر می‌شود که «بزرگ‌ترین سد راه کیست؟». قسمت ارتباطات به‌عنوان سد راه شماره یک در برابر برنامه آگاهی‌رسانی امنیتی شناخته شده‌است.



نکته جالب اینجاست که قسمت ارتباطات با بزرگ‌تر شدن شرکت، مخصوصا شرکت‌هایی با ۱۰۰۰ کارمند و یا بیشتر، سد راه بزرگ‌تری می‌شود. این امر تا حدودی مرتبط با این واقعیت است که شرکت‌های کوچک معمولا دارای قسمت ارتباطات و یا قوانین تعریف‌کننده فرایندهای ارتباط داخلی نیستند.

بزرگ‌ترین سد راه بر اساس اندازه شرکت



پس ما دارای افرادی متخصص و فنی هستیم که به یک قسمت تخصصی و فنی که کارش ارتباط با سایر قسمت‌های شرکت است، پاسخ‌گو هستند که خود یکی از بزرگ‌ترین سد راه‌های برنامه آگاهی‌رسانی امنیتی است. آیا می‌بینید که مشکل از کجاست و چرا برنامه‌های آگاهی‌رسانی امنیتی شکست می‌خورند؟

پیشنهاد

تیم آگاهی‌رسانی امنیتی خود را برای موفقیت آماده کنید. با اینکه اکثر تیم‌های آگاهی‌رسانی امنیتی از کارهایی که باید انجام شود باخبر هستند، اکثر آنها نمی‌دانند که چگونه آنها را انجام دهند. از اینکه اعضای تیم‌تان از مهارت‌هایی مانند ارتباطات، مدیریت تغییر، نظریه آموزش و مدل‌سازی رفتار برخوردارند اطمینان حاصل کنید.

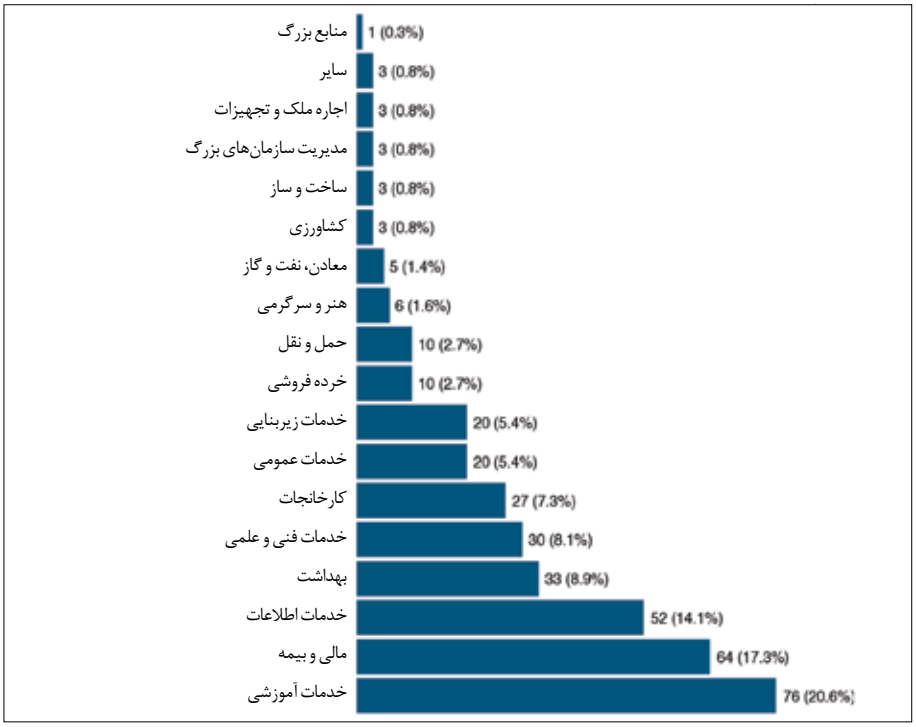
ارتباطات: نظر ما این است که ارتباطات یکی از اصلی‌ترین مهارت‌ها است. منظور ما از ارتباطات، توانایی ارسال پیام‌های بامعنی به افراد، نهایت استفاده از روش‌های ارتباطی و ساخت مسیری برای پیوند این دو است. در واقع نقش‌هایی مانند مامور امنیت ارتباطات در حال به وجود آمدن در شرکت‌ها هستند. یک راه، قرار دادن یکی از اعضای قسمت ارتباطات شرکت در تیم آگاهی‌رسانی امنیتی خود است. راه دیگر آموزش نیروهای آگاهی‌رسانی امنیتی خود با تاکید اولیه بر مقوله ارتباطات است. راه سوم، استخدام کسی با مهارت‌های مورد نیاز تان است. بدون توجه به مسیر انتخابی تان، در همان ابتدای برنامه آگاهی‌رسانی امنیتی، قسمت ارتباطات را درگیر کنید. هرچه قسمت ارتباطات زودتر در برنامه شما حضور داشته‌باشد، نیروی توانمندتری خواهدبود.

مشارکت: برنامه آگاهی‌رسانی امنیتی خود را با توضیح این امر که چرا افراد باید به این برنامه اهمیت دهند، شروع کنید. به جای استفاده از آمار و ارقام برای تفسیر نیاز به امنیت سایبری از طریق احساسی وارد شوید. به جای تبدیل کارکنان به هدف اطلاعاتی با استفاده از مکالمات و مشارکت‌های موثر، آنها را تبدیل به اعضای فعال در زمینه آگاهی کنید.

آمارگیری و اطلاعات بیشتر

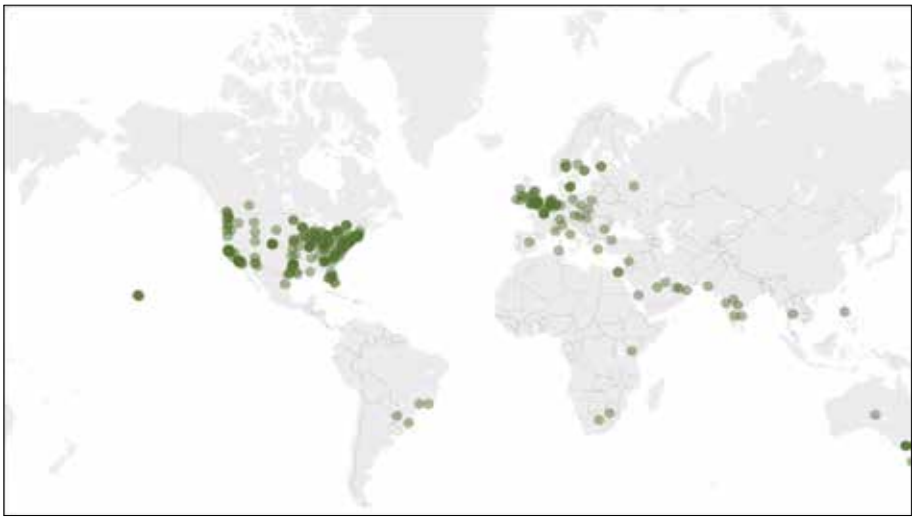
بیایید نگاهی به کسانی که در این نظرسنجی شرکت کرده‌اند، بیندازیم. اول اینکه چه صنایعی از برنامه آگاهی‌رسانی امنیتی استفاده می‌کنند؟ به‌دلیل اینکه داده‌های این نظرسنجی فقط برای ۲ سال است، نمی‌توان مطمئن بود که آیا داده‌ها نماینده صنایعی است که از برنامه آگاهی‌رسانی امنیتی استفاده می‌کنند یا اینکه فقط در رابطه با کسانی است که نظرسنجی را انجام داده‌اند. بزرگ‌ترین تفاوت امسال شمار بالای پاسخ‌دهندگان آموزشی است (۲۰٫۶ درصد).

ما امسال با استفاده از این نظرسنجی، نه‌تنها به جامعه امنیتی، بلکه به صنایع مختلف از جمله جامعه آموزش و پرورش با استفاده از انجمن EDUCAUSE دسترسی داشتیم. EDUCAUSE، انجمن آی‌تی مخصوص جامعه آموزش و پرورش است. نمودار پایین به این معنی نیست که دانشگاه‌ها بیشترین تاثیر بر برنامه آگاهی‌رسانی امنیتی داشته‌اند، بلکه نشانگر این است که EDUCAUSE باعث ترویج این نظرسنجی در جامعه آموزشی شده‌است. ما در سال آینده تصمیم داریم این نظرسنجی را حتی گسترده‌تر کرده و وارد صنایع و قسمت‌های دیگر نیز شویم.



علاوه‌بر صنایع و نواحی، ما می‌خواهیم میزان جهانی‌بودن این نظرسنجی را بدانیم. سال گذشته بیشتر شرکت‌کنندگان مؤسسات آمریکایی بودند. امسال ما دسترسی جهانی را بهبود بخشیده و باعث شدیم تا ۷۰ درصد از شرکت‌کنندگان آمریکایی و ۳۰ درصد آنها خارج از آمریکا باشند. هدف ما در سال آینده دسترسی به جوامع گسترده‌تر و جهانی‌تر است.

شرکت‌کنندگان در نظرسنجی بر اساس کشور



درنهایت باید پرســـید یک برنامه متوســـط آگاهی‌رسانی امنیتی چقدر به بلوغ رسیده‌است؟ همان‌طور که پیش‌تر به آن اشاره شد، ما میزان بلوغ را با استفاده از مدل بلوغ آگاهی‌رسانی امنیتی تعریف می‌کنیم. ۳۳ درصد از شرکت‌ها به‌تازگی برنامه آگاهی خود را آغاز کرده و یا از این برنامه در راستای پیروی از قوانین استفاده می‌کنند. ۵۱ درصد دارای برنامه‌هایی هستند که در حال تغییر رفتار افراد بوده که نسبت به آمار ۳۹ درصدی سال گذشته بهبود یافته‌است. تنها ۲ درصد مؤسسات به‌طور کامل به بلوغ در این زمینه رسیده‌اند. چراکه هم رفتار را تغییر داده و هم فرهنگ‌سازی را انجام داده‌اند و به‌علاوه دارای معیارهایی برای اثبات این قضیه هستند.

میزان بلوغ برنامه‌های آگاهی‌رسانی امنیتی

داده‌ها حاکی از بلوغ بیشتر برنامه‌های آگاهی‌رسانی امنیتی نسبت به سال گذشته هستند اما همچنان راه زیادی برای بلوغ کامل در این زمینه باقی است. چالش اصلی بیشتر مؤسسات پا را فراتر از تغییر رفتار خواهد گذاشت و به جای آن، این چالش تبدیل به ایجاد فرهنگ‌سازی و ایجاد معیارها برای نشان دادن میزان موفقیت خواهدشد.

نتیجه

با وجود اینکه مقوله آگاهی‌رسانی امنیتی در ابتدای تکامل است، نشانه‌هایی از بلوغ در این امر در حال نمایان‌شدن است. مؤسسات و شرکت‌ها نسبت به سال گذشته دارای پشتیبانی نسبتا بیشتری شده‌اند و متوسط میزان بلوغ این برنامه‌ها بهبود داشته‌است. به‌علاوه ما به شناخت خوبی از چالش‌هایمان و طریقه برطرف کردن آنها رسیده‌ایم. درنهایت باید گفت که برنامه آگاهی‌رسانی امنیتی مبحث دشواری است. این دشواری‌ها را می‌توان به‌صورت زیر دسته‌بندی کرد:

پشتیبانی ضروری است: برنامه‌های آگاهی‌رسانی امنیتی پشتیبانی لازم را برای موفقیت ندارند. بیش از ۵۰ درصد شرکت‌کنندگان در این نظرسنجی دارای بودجه‌ای کمتر از ۵ هزار دلار بوده و یا اطلاعی از میزان بودجه خود ندارند. کمتر از ۱۵ درصد از کارکنان آگاهی‌رسانی امنیتی به‌صورت تمام‌وقت روی این مقوله فعالیت می‌کنند. هرچند این امر از آمار ۱۰ درصدی سال گذشته بهتر است اما ما معتقدیم همچنان بسیار آمار کمی است. در حقیقت گزارش‌ها نشان می‌دهد که ۶۴ درصد از افراد کمتر از یک‌چهارم زمان خود را صرف این مقوله می‌کنند.

درنهایت ۳۵ درصد افراد گزارش کرده‌اند که پشتیبانی اجرایی لازم را ندارند. چرا این داده‌ها مهم است؟ به این دلیل که ارتباط مستقیم میان پشتیبانی و بلوغ برنامه آگاهی‌رسانی امنیتی را نشان می‌دهند. ما نیاز به آموزش سیستم مدیریت داریم تا بتوان به آنها نشان داد که در مقوله امنیت تنها راه حل تکنولوژی کافی نیست، بلکه فاکتور نیروی انسانی نیز باید در نظر گرفته شود. مراحل کلیدی رسیدن به این مهم شامل دو قسمت است. ابتدا اینکه برای سیستم مدیریت آشکار کنید که شما راهی اثبات‌شده برای رسیدن به فرهنگ‌سازی مورد نیاز در زمینه امنیت دارید و به‌علاوه دارای معیارهای مورد نیاز برای نشان دادن میزان تاثیر برنامه آگاهی‌رسانی امنیتی خود هستید.

کمبود مهارت: سال گذشته گزارش‌ها نشانگر کمبود مهارت در کارکنان آگاهی‌رسانی امنیتی بود. منظور از مهارت به‌طور کلی مهارت‌هایی از جمله ارتباطات، مدیریت تغییر، نظریه آموزش و رفتار انسانی است. امسال نیز داده‌ها، گزارش‌های مشابهی را در این زمینه ارائه می‌دادند.

بیش از ۸۰ درصد کارکنان آگاهی‌رسانی امنیتی دارای پیش‌زمینه‌های فنی با مهارت‌هایی از جمله توانایی اشکال‌زدایی ترافیک شبکه، ساخت وب‌سایت و یا امنیت سرور هستند. با این حال این بدان معنی است که بسیاری از اعضای تیم آگاهی‌رسانی امنیتی، درکی از مفاهیم اثبات شده و تکنیک‌های تغییر رفتار و فرهنگ ندارند. به‌علاوه از نظر ما توانایی ارتباط یکی از اصلی‌ترین مهارت‌هایی است که کمبود آن احساس می‌شود.

منظور ما از توانایی ارتباط، جذب افراد با استفاده از پیام‌ها پرمعنی، ارسال محتوای مناسب به افراد درست، نهایت استفاده از روش‌های ارتباطی مختلف و ساخت مسیر برای پیوند تمامی این موارد است. یک راه موفقیت، گماردن یکی از اعضای قسمت ارتباطات در تیم آگاهی‌رسانی امنیتی خود است. راه دیگر، آموزش مهارت‌های لازم به تیم آگاهی خود است. راه سوم استخدام فردی دارای مهارت است. خلاصه اینکه شما علاوه‌بر کارشناسان امنیت، نیازمند به افرادی با مهارت‌های ارتباطی در تیم آگاهی خود هستید

منبع: موسسه SANS

مترجم: حسین رسولی