

پنج گام به سوی یک برنامه استراتژیک کارآمد

Stan Gatewood، مدیر ارشد امنیت اطلاعات دانشگاه جورجیا، اهداف امنیتی را بر اساس انطباقشان با اهداف و استراتژی عمده دانشگاه سازماندهی می نماید. وی دلایل متعددی برای این امر که چرا مدیران ارشد امنیت اطلاعات نباید خود را برای برنامه ریزی استراتژیک به زحمت بیاندازند، دارد. فقط کافیسیت برسید.

Stan Gatewood، مدیر ارشد امنیت اطلاعات دانشگاه جورجیا، اهداف امنیتی را بر اساس انطباقشان با اهداف و استراتژی عمده دانشگاه سازماندهی می نماید. وی دلایل متعددی برای این امر که چرا مدیران ارشد امنیت اطلاعات نباید خود را برای برنامه ریزی استراتژیک به زحمت بیاندازند، دارد. فقط کافیسیت برسید. مدیر ارشد امنیت اطلاعات دانشگاه جورجیا، می گوید: "شما مسئله اقتصاد را دارید که در مقابل شما نقش ایفا می کند. شما دارای رفتار اجتماعی هستید که در مقابل شما نقش ایفا می نماید. شما تکنولوژی را دارید. شما قوانین و مقررات را در پیش رو دارید." و خود را برای یافتن کتاب ها یا سمینارهای تخصصی در جهت کمک به شما برای اعمال اصول برنامه ریزی استراتژیک تجاری در امنیت به زحمت نیاندازید. چون چیزی نخواهید یافت .

علی رغم همه این موارد، Gatewood اینجاست تا بگوید که شما به انجام برنامه ریزی استراتژیک نیاز دارید. او می پرسد: "اگر شما هیچ برنامه ای نداشته باشید، چگونه متوجه خواهید شد که آن را به درستی انجام می دهید؟" او این گونه ادامه می دهد: "شما در برابر هر چیز کوچکی که در شب تکان می خورد عکس العمل نشان خواهید داد." نهایتاً، این روشی بوده که اغلب گروه های امنیت اطلاعات سال ها بر اساس آن عمل کرده اند: شیشه را بشکن، دستگیره را بکش. دپارتمان های امنیت به دشواری می توانستند آینده خود را کنترل نمایند، زمانی که راهبری آنها بیش از حد بر اساس حوادث بود، این ایده کاربرد خود را از دست داد. اما همه این ها در حال تغییر است، همچنان که مدیران ارشد امنیت و مدیران ارشد امنیت اطلاعات شروع به مد نظر قرار دادن ارزش استفاده از اصول شناخته شده ی برنامه ریزی استراتژیک برای راهبری تلاش خود نموده اند. در اساس خود، برنامه ریزی استراتژیک چیزی بیش از یک فرایند رسمی برای تنظیم اهداف بر اساس منظورهای تجاری و سپس مشخص کردن شیوه دستیابی به این اهداف نیست – البته در طی سال های پیش رو، نه ماه ها .

مطمئناً، بسیاری از شما دارای سیاست های بلندپروازانه ای هستید. و مطمئناً، اغلب شما دارای برنامه های تاکتیکی در راستای بودجه هایتان برای سال پیش رو هستید. به هر حال، یک برنامه استراتژیک خوب، در مکان مطبوعی میان این دو سطح قرار می گیرد. مدیران ارشد امنیت که نحوه ایجاد و پیاده سازی یک برنامه تاکتیکی را درک نموده اند مدعی اند که این امر در استفاده خردمندانه از منابع، جلب پشتیبانی برای طرح های امنیتی و نائل شدن به هم تراز با تجارت به آنها کمک می نماید. هیچ شیشه ای شکسته نشده است James، Quinnild، یک همکار امنیتی در طرح مشورتی در PricewaterhouseCoopers، می گوید: "در مورد مدیر ارشد امنیت، ارشدیت اهمیت ویژه ای دارد. مدیران ارشد امنیت سرمایه های بیشتری را اداره می کنند، سطح میدان دید آنها درون سازمان بسیار بالاتر است، و افراد بیشتری مدیر ارشد امنیت را مورد پرس و جو قرار می دهند، کارها چطور پیش می رود؟ مشغول انجام چه کاری هستید؟ آیا کارهای خود را اولویت بندی می نمایید؟ یک برنامه خوب طراحی شده در پاسخگویی به این سوالات مفید واقع می شود .

به خصوص در حوزه امنیت اطلاعات که به سرعت در حال تغییر است، برنامه ریزی برای آینده می تواند مخاطره آمیز باشد. تکنولوژی ها تغییر می کنند، و تهدیدات جدید پدیدار می شوند. اما در مقابل این چالش ها، در صورتی که شما خواهان خارج ساختن سازمان خود از حالت بحرانی هستید، فرایند برنامه ریزی استراتژیک یک امر حیاتی است. در ادامه پنج گام برای آغاز کار مطرح می گردد. همان گونه که مشاهده خواهید نمود، این یک روند محرمانه نیست. این Business ۱۰۱ است، که در حوزه امنیت اعمال گردیده است .

۱ (کار را با برنامه تجاری دارای چشم انداز وسیع آغاز نمایید

هنگامی که Gatewood دو سال پیش کار خود را در دانشگاه جورجیا آغاز کرد، یکی از نخستین کارهایی که انجام داد مطالعه همه برنامه های تجاری برای دانشگاه بود که او می توانست مورد استفاده قرار دهد. مهمترین مورد؟ یک برنامه پنج ساله که توسط رییس دانشگاه (که بیش از ۳۳۰۰۰ دانشجو داشت) نوشته شده بود. این نوع رویکرد با چشم انداز وسیع و طولانی مدت می تواند به مدیر ارشد امنیت در خارج شدن از وضعیت تاکتیکی یاری برساند Gatewood. می گوید: "من نقطه ای که دانشگاه قصد رسیدن به آن را داشت دیدم، و سپس کار ایجاد اهداف استراتژیک امنیتی را بر مبنای آن آغاز کردم."

برای نمونه، یکی از اولویت های رییس جذب استادان رده بالا و عالی بود Gatewood. اطمینان حاصل نمود که برنامه های دپارتمان او انعکاس دهنده همین هدف باشد Gatewood. می گوید: "اگر شما پا پیش بگذارید و بگویید، 'من برای یک فایروال جهت حفاظت از گروه تحقیقات به ۵۰۰۰۰ دلار نیاز دارم' این کافی نیست." در عوض، او اهداف خود را بر اساس مطابقتشان با اهداف و استراتژی عمده دانشگاه سازماندهی می نماید. او می گوید: "من این سوال را مطرح کردم: شما چگونه می توانید یک استاد را برای انجام تحقیقات پیشرفته جذب نمایید در صورتی که تکنولوژی مورد استفاده او قابل اعتماد نباشد؟" گاهی اوقات یک تغییر معنایی می تواند تفاوت بزرگی ایجاد نماید. به هر حال، فقط مطالعه استراتژی تجاری کافی نیست. شرکت دادن افراد تجاری در فرایند برنامه ریزی تضمین می نماید که امنیت در مسیر درست پیش می رود و همچنین به شما در جذب پشتیبانی برای برنامه تان کمک می کند Bobby Gillham، رییس سابق امنیت ConocoPhillips که اکنون یک مشاور است، می گوید: "کسب و کارها بودجه های ثابتی دارند و همچنین محدودیت هایی در مورد کارهایی که می توانند انجام دهند و کارهایی که نمی توانند. شما مجبورید اینها را متقاعد نمایید که یک پیشرفت امنیتی واقعا جزو بهترین موارد مورد علاقه کسب و کارها به شمار می آید، و این که آنها در مورد پرداخت پول برای آن راضی و موافق هستند."

Gillham می گوید، با نگاه به پیشرفت هایی که قصد دارید در طی سه سال آینده به آنها نائل آید به جای این که تنها نگاهتان به چرخه بودجه جاری باشد، ممکن است شما توانایی متقاعد ساختن رؤسای تجاری نسبت به دادن التزام طولانی مدت تر در قبال یک پروژه خاص را داشته باشید. اگر یک دپارتمان خاص در بودجه خود برای سال مالی آتی برای پروژه شما پول ندارد، شاید بتوانید گروه را نسبت به گنجاندن آن برای سال بعد متقاعد نمایید. حتی این احتمال وجود دارد که راهی برای بسط هزینه در طی چندین سال بیابید. در پیش گرفتن یک چشم انداز طولانی مدت اغلب می تواند به عملی شدن اهدافی که نمی توانند در بودجه یک ساله بگنجد کمک کند .

۲ (همواره یک ارزیابی ریسک انجام دهید

هنگامی که از اولویت های تجاری آگاهی یافتید، گام بعدی درک این مطلب است که چه ریسک های امنیتی ممکن است مانع دستیابی کسب و کار به اهداف گردد. این کار با یک ارزیابی ریسک صورت می پذیرد. در **Avon Products**، این فرایند چهار ماه قبل از این که **Robert Littlejohn**، قائم مقام مدیرعامل در امنیت جهانی، مدیران رده بالای خود را برای یک نشست استراتژی سالانه دو روزه گرد هم آورد آغاز گردید. با آغاز در ماه ژوئن، از سرتاسر جهان مدیران امنیت منطقه ای فرم هایی را برای مدیران تجاری **Avon** ارسال می نمایند تا از آنها برای ارزیابی ریسک هایی که در پیش روی آنها قرار دارد استفاده گردد. از مدیران تجاری خواسته شده است که احتمال وقوع هر رویداد و تاثیر بالقوه آن بر شرکت (که در ۱۴۵ کشور مشغول به فعالیت است) را برآورد نمایند. در ماه آگوست، این ارزیابی ریسک توسط یک نظرخواهی مشتری در این مورد که مدیران تجاری فرایندهای ریسک سازمانی و امنیتی را چگونه می بینند همراهی خواهد شد: چه چیز نتیجه می دهد؟ چه چیز نتیجه نمی دهد؟ مهمترین دغدغه های آنها چیست؟

سپس مدیران امنیت منطقه ای به بررسی دقیق ارزیابی ریسک می پردازند تا اعتبار آن را مورد تایید قرار دهند، تغییراتی را در آن اعمال نمایند یا در صورت لزوم مواردی را به آن بیافزایند. برای نمونه، **Littlejohn** به یاد می آورد که سال گذشته، یک مدیر تجاری در مورد شرکتی نشان داد ریسک بالایی وجود دارد که ورشکست گردد. مدیر امنیت منطقه ای به شرکت مراجعه کرد، با مدیر امنیت منطقه ای و مدیر آن شرکت به همفکری پرداخت، و مشخص گردید که از آن چه که مدیر تجاری نشان داده بود، این شرکت با ثبات تر است. تنها چیزی که می توان گفت این است که اگر چه باید مدیران تجاری را در فرایند برنامه ریزی شرکت داد، اما در برخی موارد به وجود یک متخصص امنیت برای تایید اعتبار ارزیابی ریسک نیاز است.

این مهارت، اتفاقاً می تواند خارج از برنامه ریزی استراتژیک دپارتمان امنیت حاصل گردد. می تواند مدیر ارشد امنیت را در طی برنامه ریزی استراتژیک تجاری نیز به فردی فوق العاده با ارزش تبدیل نماید **Paul Laudicina**، یک قائم مقام مدیرعامل **A.T. Kearney** و مدیر **Global Business Policy Council** که **World Out of Balance** را نوشته است **Navigating Global Risks to Seize Competitive Advantage**، بر این عقیده است که شرکت هایی که خواهان کسب موفقیت در بازار جهانی هستند باید در مورد اداره همه انواع ریسک فهیم تر و زرنگ تر باشند - از بیماریهای مسری و واگیردار گرفته تا اپیدمی ها، تا ویروس های کامپیوتری. یک مدیر ارشد امنیت می تواند در این فرایند نقش حیاتی داشته باشد. یا اصلاً نقشی نداشته باشد **Laudicina** می گوید: "در هر صورت مدیریت این ریسک ها وظیفه مدیر ارشد امنیت است یا شخص دیگری باید تعیین نماید که آیا مدیر ارشد امنیت قادر به نیل به اهداف است."

۳ (اهداف قابل سنجش را برای گروه خود تعیین نمایید، تا برنامه خود را استوار نگه دارید

هنگامی که وظیفه خود را انجام دادید، نوبت به پیوند دادن اهداف و ریسک های تجاری است. شما نیازمند استراتژی خودتان هستید. در بالاترین سطح، اهداف شما قرار دارند. آنها می توانند به همان سادگی که شما می خواهید باشند **Littlejohn** در شرکت **Avon** یک وظیفه آسان بر عهده دارد: حفاظت از کارکنان، محصولات، منافع، دارایی ها، فرایندها، و اعتبار **Avon** در **AT&T**، اهداف **CISO Ed**

Amoroso به همین میزان ساده است: بهبود امنیت، کاهش هزینه ها، و استفاده از امنیت برای برقرار ساختن تفوق رقابتی. (فقط مدیر ارشد اجرایی AT&T را در حال سر و کله زدن با هر یک از آنها تصور کنید، مهم نیست که استراتژی کلی این غول ارتباطی با چه عظمتی در حال تغییر است.)

استراتژی، راهی است که شما از آن طریق این وظایف را در طی سال های آتی انجام می دهید. هر چه برنامه جلوتر می رود، جنبه های خاص و جزئیات آن کمتر می گردد. همچنین، شما ممکن است این روند را برگزینید که یک برنامه دارای جزئیات کمتر را با هیئت مدیره شریک شوید و یک برنامه مفصل تر داشته باشید که آن را در دپارتمان امنیت بخشنامه نمایید. ترفند این است که برای سال آینده فراتر از تاکتیک های خود بنگرید و اهداف خود را برای سال های پیش رو مجدداً شکل دهید. برای نمونه، یک برنامه تاکتیکی ممکن است چگونگی اداره برنامه های اصلاحی نرم افزاری برای آینده نزدیک از سوی دپارتمان امنیت را در بر گیرد. اما بخش استراتژیک مدیریت برنامه های اصلاحی (patch)ها بسیار متفاوت است، منوط به این که مدیر ارشد امنیت اطلاعات پیش بینی نماید که برای چه مدتی مدیریت جدی برنامه های اصلاحی لازم خواهد بود .

Amoroso می گوید: "اگر ما به این نتیجه می رسیدیم که صنعت نرم افزار در دو یا سه ماه آینده به باگ دیگری در نرم افزارهای خود بر نخواهد خورد، در آن صورت ما تصمیم به سرمایه گذاری برای یک زیربنای patch نمی گرفتیم. درون من به من می گوید که این وضعیت در دو ماه آینده بهتر نخواهد شد. اما سوال اینجاست که چه وقت این اتفاق خواهد افتاد؟" اگر مدیر ارشد امنیت اطلاعات پیش بینی نماید که گروه او در طی پنج سال آینده مجبور به نصب تعداد فراوانی برنامه اصلاحی باشد، شاید به این نتیجه برسد که برای ادامه این راه و کارآمد سازی فرایند نصب نیاز به بودجه وجود دارد. اما اگر او به این نتیجه برسد که برنامه های اصلاحی یک راه حل موقتی هستند و فروشندگان نهایتاً محصولات بهتری را تولید خواهند نمود، شاید او یک تصمیم استراتژیک مبنی بر انجام patch ها به صورت دستی اتخاذ نماید.

نویسنده Sarah D. Scalet :

مترجم: امین ایزدپناه