کد خبر: ۴۰۲۳۹۱
سه شنبه ۳۱ خرداد ۱۴۰۱ ۱۴:۵۹

امن‌سازی زیرساخت‌های «افتا» در مقابل حملات سایبری دشمن

یافتن پاسخی مناسب به این پرسش بسیار دشوار است، زیرا اطلاعات موجود ناچیز بوده و اغلب از سوی منابعی ارائه شده اند که بی طرفی آن ها مورد تردید است.<;br&#۴۷;><br&#۴۷;>

به گزارش سایت خبری پرسون، سجاد عابدی در یادداشتی نوشت: در واقع نمی توان به سادگی شدت حقیقی خطرات سایبری را (یا به عبارت دیگر اقدامات خصمانه دائمی ای که سیستم های اطلاعاتی در سطح جهان را تحت تاثیر قرار می دهند) به طور قطع تعیین کرد.

رکن اصلی امنیت سایبری – از ابتدای توسعه این مفهوم، - اجرای تدابیر فنی و غیر فنی ای است که امنیت سیستم های اطلاعاتی را تضمین می کنند. اما برای آنکه این تدابیر تاثیرگذاری داشته باشند، باید تمامی تهدیدات و آسیب پذیری های ممکن را پوشش دهند، چرا که تنها یک نقص کوچک می تواند بستر حمله ای گسترده را فراهم کند.

در عصر اطلاعات شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی از قبیل اطلاع‌رسانی، ارائه خدمات، مدیریت و کنترل ارتباطات، از طریق سازوکارهای فضای مجازی انجام می‌پذیرد. این فضا که از آن با نام "فضای تولید و تبادل اطلاعات" یاد می‌شود، در معرض چالش‌ها، آسیب‌ها و تهدیدات گوناگونی نظیر ارتکاب جرائم سازمان‌یافته، حملات مختل‌کننده خدمات، جاسوسی، خرابکاری، تخریب بانک‌های اطلاعاتی، نقض حریم خصوصی و نقض حقوق مالکیت معنوی قرار دارد.

تهدیدات امنیتی فضای مجازی با سوءاستفاده از پیچیدگی و اتصال روزافزون سیستم‌های موجود در سازمان‌ها و به‌ویژه زیرساخت‌های حیاتی، حساس و مهم، مواردی همچون امنیت، اقتصاد، ایمنی و سلامت عموم را در معرض خطر قرار می‌دهند. حفاظت از زیرساخت‌های حیاتی ملی برای ایجاد جامعه‌ای امن، ایمن و مقاوم در قبال حملات سایبری و سایر مخاطرات طبیعی و انسانی امری ضروری است. در این راستا زیرساخت‌های حیاتی نیازمند سازوکارهایی برای حفظ محرمانگی، یکپارچگی و دسترس‌پذیری دارایی‌های خود می‌باشند. با توجه به نوپایی مفهوم امنیت فضای تولید و تبادل اطلاعات و با عنایت به میزان تأثیر آن بر امنیت ملی کشور، پرداختن به این موضوع و نهادینه‌سازی آن به‌عنوان یک ضرورت و اولویت تلقی می‌شود.

هدف از این طرح، تأمین امنیت فضای تولید و تبادل اطلاعات سازمان و جلوگیری از بروز اختلال در ارائه سرویس‌های حیاتی آن است. در این طرح الزاماتی برای ایجاد، پیاده‌سازی، نگهداری و بهبود مستمر امنیت اطلاعات در حوزه‌های زیرساختی ارائه‌شده است. همچنین سازمان نیازمند ساختاری برای تأمین منابع انسانی و مالی به‌منظور اجرای طرح است. این ساختار متناسب با شرایط و اهداف سازمان می‌تواند در قالب کمیته اجرای طرح یا ایجاد واحدی سازمانی باشد. تشکیل این ساختار به‌عنوان پیش‌نیازی برای اجرای سایر الزامات طرح بوده و پس از انجام اقدامات فوق در سازمان، لازم است طرح امن‌سازی متناسب با نقشه راه اجرایی گردد.

راهبرد اصلی طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری، مدیریت مخاطرات است. مدیریت مخاطرات فرآیندی مستمر است که در آن تهدیدات و آسیب‌پذیری‌های موجود در یک سازمان شناسایی و ارزیابی می‌شوند و از طریق انجام اقدامات امن‌سازی که اولویت بیشتری دارند، مخاطرات مدیریت می‌شوند. لازمه این امر وجود یک رویکرد مدیریت مخاطرات سیستماتیک متناسب با بافتار، شرایط و مخاطرات خاص سازمان است که بدین منظور، امروزه استانداردها و روش‌های متعددی نظیر ISA/IEC ۶۲۴۴۳، ISO ۳۱۰۰۰، ISO/IEC ۲۷۰۰۵ و ... چارچوب‌های مناسبی را برای مدیریت مخاطراتی که به امنیت اطلاعات لطمه می‌زند در اختیار سازمان‌ها قرار می‌دهند. سازمان باید مدیریت مخاطرات امنیت را مطابق با الزامات شکل زیر تعیین نماید.

زیرساخت محرمانگی و استناد پذیری نیازمند تدوین سیاست‌ها، ضوابط، رویه‌ها در بعد مدیریتی و بهره‌گیری از ابزارهای امنیت اطلاعات و ارتباطات در بعد فنی بوده که محرمانگی اطلاعات را برای سازمان تضمین می‌نماید. قلمرو این زیرساخت در بعد فنی شامل الگوریتم‌های رمزنگاری، پروتکل‌های امنیتی، زیرساخت کلید عمومی و... است. لزوم استقرار زیرساخت محرمانگی و استناد پذیری در سازمان، جلوگیری از افشاء داده‌ها و اطلاعاتی است که باید محافظت شوند و در اختیار افراد غیرمجاز قرار نگیرند. تمامی کاربردهای زیرساخت محرمانگی و استناد پذیری در بستر زیرساخت کلید عمومی قابل تحقق است.

هر نوع داده یا مبادله الکترونیکی مطرح در حوزه عملیات خصوصی و غیرخصوصی که تهدید امنیتی در مورد آن مطرح باشد، جزء مواردی است که می‌توان از زیرساخت کلید عمومی برای امن سازی آن بهره گرفت. از موارد پرکاربرد زیرساخت محرمانگی سازمان‌ها می‌توان به مدیریت کلیدهای رمزنگاری، امن‌سازی کاربردهای تحت وب، امن‎سازی برنامه اتوماسیون اداری، تصدیق هویت و ... اشاره نمود.

پس از پیاده‌سازی و اجرای برنامه‌های عملیاتی تدوین‌شده، باید از اجرای اثربخش برنامه مذکور اطمینان حاصل گردد. در این راستا ضروری است ممیزی‌های مستمر و ادواری در سازمان انجام شود. لذا مرکز افتا (امنیت فضای تولید و تبادل اطلاعات) موظف است تا کلیه ممیزی‌ها را بر اساس ابزار ارزیابی سطح بلوغ ارائه‌شده، مدیریت و سازمان را از نتیجه مطلع نماید.

ممیزی داخلی: سازمان باید روال‌های مشخصی را برای برگزاری ممیزی داخلی تدوین کرده و به‌طور منظم نسبت به برگزاری آن‌ها اقدام کند. جهت اطمینان از اجرای الزامات، سازمان گزارش‌های لازم را بر اساس فرم‌های ممیزی مرکز افتا تهیه و جهت بررسی و اخذ تأییدیه به مرکز افتا ارسال می‌نماید.

ممیزی خارجی: جهت نظارت بر روند اجرای برنامه‌های عملیاتی و اثربخشی آن‌ها ممیزی خارجی توسط مرکز افتا انجام خواهد شد. سازمان پس از اخذ گزارش‌های ممیزی خارجی، نسبت به رفع انطباق‌ها اقدام نموده و در صورت نیاز، درخواست ممیزی مجدد از مرکز افتا را خواهد نمود.