عنوان مقاله:
یک مدل مفهومی برای کاهش مخاطرات در مقابل حملات سایبری

محل انتشار:
سومین کنفرانس ملی در مهندسی کامپیوتر، فناوری اطلاعات و پردازش داده ها (سال: 1397)

تعداد صفحات اصل مقاله: 15

نویسنده:
مهدی بشیری - *دانشگاه علمی کاربردی تهران واحد علمی نور*

خلاصه مقاله:
برای جلوگیری از به خطر افتادن تداوم کسب و کار بواسطه آسیب پذیریهای موجود در شبکه و سامانه ها، درک مناسب اهداف و الزامات امنیت اطلاعات سازمان و لزوم ایجاد خط مشی، پیاده سازی و اجرای کنترلها برای مدیریت امنیت اطلاعات، حفظ زیرساخت فناوری اطلاعات و ارتباطات در مقابل حملات سایبری، بهبود کسب و کار بر پایه نظارت مستمر، حفاظت خودکار زیرساخت فناوری اطلاعات، افزایش بهره وری و کاهش هزینه های موجود در فناوری اطلاعات و در نهایت مستند نمودن سیاستهای امنیتی برای طبقه بندی داده ها نیاز به مدل مفهومی کاربردپذیر و قابل اجرا میباشد را ضروری مینماید.وجود استانداردهای امنیتی از قبیل سری استانداردهای بین المللی سری ۲۷۰۰۰، گزارشهای فنی سری ۱۳۰۰۰ و استانداردهای موسسه ملی فناوری و استانداردها مفید میباشند، اما به دلایلی از قبیل طولانی بودن، پیچیدگی های منحصربفرد و نامفهوم بودن و همچنین زمان بر و طولانی شدن فرایند طراحی، ایجاد و پیاده سازی آنها در مدیریت امنیت اطلاعات و تهیه اسناد مرتبط ناکارآمد نشان میدهد.به رغم دستاوردهای مختلف و وجود استانداردهای امنیتی، دستورالعملها و روشهای برتر، فضای سایبری دارای چالشها و مسایلی از قبیل به خطر افتادن کسب و کار، عدم ارایه سرویس، نشت اطلاعات و نفوذ خرابکارها و بروز اختلال در سرویسهای حیاتی و وجود باجافزاها میباشد، که ضمن وارد کردن و صرف هزینه ها گزاف و اتلاف وقت سازمان، از کارآمدی مطلوبی برخوردار نمی باشد.لذا ما در این مقاله یک مدل مفهومی پیشنهاد کرده ایم تا با ارایه و ایجاد مدلی مفهومی بر پایه استانداردهای موجو، اقداماتی شامل شناسایی، حفاظت، تشخیص، پاسخ و بازیابی تعریف و ایجاد نماییم. تا بتوان کنترلهای امنیتی مناسبی برای پوشش کامل و تسهیل در اجرای هر یک از اقدامات ایجاد شده که ضمن کاربردپذیری، اجرا و قابلیت پیاده سازی، کارایی مناسبی داشته باشند و حداقل اصول زیر را پوشش دهد، ایجاد نماییم: (۱ تمرکز بر نظارت مداوم برای تست و ارزیابی اصلاح؛ (۲ فرایندهای خودکار برای رسیدگی به امنیت با کارایی، قابلیت اطمینان و مقیاس پذیری؛(۳ ارایه معیارهای مشترک، که به تمام ذینفعان اجازه می دهد به طور عینی اقدامات امنیتی را ارزیابی و تنظیم کنند؛ و (۴ به سازمان با استفاده از دانش و تکنیکهای حملات واقعی در ایجاد دفاع موثر کمک شایانی خواهد نمود.که با پیروی از این اصول میتوان محرمانگی، یکپارچگی و در دسترس پذیری به دارایی های فناوری اطلاعات خود را تضمین نمود. ضمن آنکه با فراهم شدن زیرساخت لازم و تبدیل مدل مفهومی به سامانه ی هوشمند، تمامی اقدامات و کنترلها بصورت سیستمی و خودکار صورت پذیرد تا اصول بیان شده را بهتر و کارآمدتر اجرا و پیاده سازی، نظارت و قابل ممیزی باشد.

کلمات کلیدی:
استانداردهای امنیتی، آسیب پذیری، حملات سایبری، استانداردهای موسسه ملی فناوری و استانداردها، طبقه بندی داده ها، امنیت سایبری، مخاطره امنیتی، شناسایی، حفاظت، تشخیص، پاسخ، بازیابی، کنترلهای امنیتی