عنوان مقاله:
ارائه رویکرد ساختاریافته برای اجرای رزمایش سایبری

محل انتشار:
اولین کنفرانس ملی چالش های مدیریت فناوری اطلاعات در سازمان ها و صنایع (سال: 1393)

تعداد صفحات اصل مقاله: 13

نویسندگان:
رحیم یزدانی - *دانشجوی دکتری،دانشگاه عالی دفاع ملی، تهران،ایران*

ناصر مدیری - *عضو هیئت علمی دانشگاه آزاد اسلامی واحد زنجان،ایران*

خلاصه مقاله:
فضای سایبریک محیط راهبردی بوده و به لحاظ کارکردها ی متنوعش مورد علاقه دولت ها و سازمان ها است که نتیجه اش افزایش تقاضا برای امن کردن این فضاست. لذا به منظور تعیین میزان آمادگی جهت حفاظت از دارائی ها و سامانه ها درقبال حملات ،تمرین تصمیم گیری مدیریتی پاسخگو،تعیین میزان تعامل سازمان بامحیط بیرون در طرح پاسخ سایبری،بررسی مسیر اشتراک گذاری اطلاعات وارتباطات درصورت وقوع حمله،تعیین سیاست هایی که امنیت سایبر را پشتیبانی می کنند،ارتقاءتراکنش ها،افزایش آگاهی های مربوط به تاثیر حوادث سایبری،برجسته سازی فناوری های مرتبط با شناسائی وبازیابی اثرات حمله ،رزمایش سایبری روش موثری در یادگیری جنبه های عملی امنیت اطلاعات است. اعضای تیم های پاسخ سریع به حوادث رایانه ای اقدام به تست مهارت،توان پاسخ دهی ،پیاده سازی روش های عملیاتی پاسخ دهی،بهبود برنامه ریزی،حفظ و تقویت همکاری های بین المللی،در قالب رزمایش های امنیت سایبری درسطح سازمانی و ملی می کنند.طراحی و اجرای رزمایش امنیتی سایبری پیچیده است زیرا فرم ها ورویکردهای مختلفی می تواند داشته باشد.دراین پژوهش ابتدا به جایگاه رزمایش در کشورمان پرداخته ، درادامه به مدل ها و پیش فرض هاوپلت فرم هاو انواع رزمایش های سایبری اشاره می کنیم. ونهایتا به نحوه برنامه ریزی و مسئولیت بخش های موثر در رزمایش و مراحل گام به گام درطراحی رزمایش می پردازیم

کلمات کلیدی:
رزمایش امنیت سایبری،مدل،مسئولیت