9th SASTech Symposium on Advances in & Science Technology (2014)
نهمین سمپوزیوم پیشرفت های علوم و تکنولوژی
مشهد- ۱۳ آذر- ۱۳۹۳
کمیسیون دوم: همایش ملی علوم و مهندسی کامپیوتر
با محوریت
امنیت ملی و توسعه پایدار
برگزارکننده: موسسه آموزش عالی خاوران
www.khi.ac.ir

رزمایش سایبری رویکردی نوین جهت آمادگی در برابر تهدیدات سایبری

محمد رضا موحدی راد[۱]، ناصر مدیری[۲]

۱- دانشجوی کارشناسی ارشد کامپیوتر نرم افزار ، دانشگاه آزاد اسلامی واحد تهران شمال

۲- استادیار دانشکده برق و کامپیوتر ، دانشگاه آزاد اسلامی واحد زنجان

mr.movahed@chmail.ir

خلاصه

فضاهای سایبری امروزی که به طور فزاینده ای خصومت آمیز شده اند شامل تهدیدات به سرعت در حال تغییری هستند که در بسیاری اوقات بر توانایی واکنش سازمان ها به این تهدیدات سبقت می گیرند. طراحی فرآیندها و راهکارهای مشترک به منظور افزایش توانایی برای دفاع در برابر تهدیدات سایبری و کاهش اثرات آن ضروری است. برنامه ریزی و اجرای رزمایش های سایبری عاملی مهم در ارتقاء این قابلیت های مشترک است. برنامه ها و راهکارهایی که از طریق برنامه ریزی و اجرای رزمایش های سایبری به وجود می آیند و تست می شوند نقش قابل توجهی در آمادگی و واکنش سایبری دارند و باعث ایجاد امنیت بیشتر در فضای سایبری می گردند.

کلمات کلیدی: رزمایش سایبری، تهدیدات سایبری، دفاع سایبری، امنیت سایبری

۱. مقدمه

فضاهای سایبری امروزی که به طور فزاینده ای خصومت آمیز شده اند شامل تهدیدات به سرعت در حال تغییری هستند که در بسیاری اوقات بر توانایی واکنش سازمان ها به این تهدیدات سبقت می گیرند. مثالی خوب در این زمینه واکنش انجمن بین المللی امنیت سایبر به کرم کنفیکر است [۱]. پنج گونهٔ این کرم بین نوامبر ۲۰۰۸ و آوریل ۲۰۰۹ شناسایی شد، که هر کدام نسبت به قبلی ارتقاء یافته بود، و با واکنش های شدیدتر انجمن امنیت سایبری مواجه شد. علاوه بر این می توان به حمله بدافزار های استاکس نت[۱] [۲] و فلیم[۲] که آسیب هایی را به سیستم های حیاتی و حساس درکشور وارد کرده اند، اشاره کرد. در مواجهه با این تغییرات سریع سازمان های دولتی و خصوصی دریافته اند که باید رویکردی پیشگیرانه تر را اتخاذ کنند. با اینکه پیشگیری

[1] Stuxnet
[2] Flame