عنوان مقاله:
شناسایی حملات و خطرات وارده بر شبکه های کامپیوتری و راهکار های امنیتی درشرکت راه آهن جمهوری اسلامی ایران

محل انتشار:
هشتمین کنفرانس بین المللی مهندسی برق، کامپیوتر و مکانیک (سال: 1401)

تعداد صفحات اصل مقاله: 18

نویسندگان:
امیرهوشنگ تاجفر - *عضو هیئت علمی دانشگاه پیام نور*

مصطفی جعفریان - *دانشجوی کارشناسی ارشد دانشگاه پیام نور*

خلاصه مقاله:
در این مقاله به راهکارهای امنیتی موثر برای جلوگیری از نفوذ در شبکه های اطلاعاتی شرکت راه آهن جمهوری اسلامی ایران که همواره در معرض تهدیدات و حملات زیادی قرار داشته و دارد می پردازیم. شرکت راه آهن ج ا ا یکی از مهم ترین مراکز کشور در زمینه حمل و نقل به شمار می رود که تهدیدات و حملات متعددی به آن صورت گرفته است. مهم ترین راهکارها در برابر حملات سایبری در شرکت راه آهن ج ا ا به ترتیب اولویت بعبارت اند از: ۱- پشتیبان گیری مداوم از داده های حیاتی و حساس ۲- مستندسازی و ارائه گزارش تهاجم های تشخیص داده شده قبلی به تیم امنیت ۳- مرور گزارش های روزانه مربوط به تجهیزات نرم افزاری و سخت افزاری (لوگ ۱) ها ۴- استفاده از سامانه های موازی ۲ ۵- استفاده از پروتکل های رمزنگاری جهت کد کردن اطلاعات مبادله شده ۶- استفاده از تیم های سی آی آرتی ۳ ۷- پیاده سازی استاندارد آی اس ام اس ۴ در سازمان ۸- تدوین سیاست های امنیتی جامع در سازمان مانند کنترل دسترسی، استفاده از رمز عبور ۹۰ آموزش ، فرهنگ سازی و آگاهی کاربران ۱۰ استفاده از سامانه اس اوسی ۵ بومی (کنترل ۲۴ ساعته ورودی ها خروجی های شبکه) ۱۱ لیست فرآیندهای انجام شده REDANDANT گروه واکنش سریع رایانه ای سامانه مدیریت امنیت اطلاعات مرکز عملیات امنیت امنیت فیزیکی مناسب و تخصیص مکان های امن برای تاسیسات ۱۲- استفاده از فن آوری های نوین بومی (نرم افزاری و سخت افزاری) براساس نتایج به دست آمده اولویت های اول تا چهارم راهکارهای ارائه شده در برابر حملات سایبری برای شرکت راه آهن ج ا.ا، جملگی بر استفاده از پشتیبان گیری، افزونگی، مستندسازی و مرور مستندات روزانه دلالت دارد و استفاده از فن آوری های بومی نرم افزاری و سخت آفزاری در اولویت آخر قرار دارد و با توجه به عقب ماندگی کشورمان در زمینه فناوری های نرم افزاری و سخت افزاری، در حال حاضر بومی سازی این دو مقوله راهکار مناسب به نظر نرسیده است و می بایست جهت خودکفایی و ارتقاء دانش فناروی اطلاعاتی (نرم افزاری و سخت افزاری) همت بیشتری در سطح کشور گمارده شود.

کلمات کلیدی:
حملات سایبری کش و نفود، مرکز عملیات امنیت ، ریسک،پویش تجهیزات