

عنوان مقاله:

تاثیر حملات سایبری بر تجهیزات صنعتی

محل انتشار:

اولین کنفرانس بین المللی جهش علوم مدیریت، اقتصاد و حسابداری (سال: 1400)

تعداد صفحات اصل مقاله: 5

نویسندگان:

محمد ملکی نیا - دکتری مدیریت فناوری اطلاعات - استاد دانشگاه آزاد اسلامی واحد تهران جنوب - استاد راهنمای مقاله

میترا معمرگنجین - دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات - گرایش سیستم های اطلاعاتی - دانشگاه آزاد اسلامی واحد تهران جنوب

حامد مشایخی - دانشجوی کارشناسی ارشد مدیریت فناوری اطلاعات - گرایش سیستم های اطلاعاتی - دانشگاه آزاد اسلامی واحد تهران جنوب

خلاصه مقاله:

امروزه کلیه زیرساخت های حیاتی، واحدهای صنعتی و آموزش و پژوهش، حمل و نقل، بهداشت و درمان و ... از سیستم های کنترل مبتنی بر شبکه استفاده می کنند. کنترل و پایش در زیرساخت های حیاتی و واحدهای صنعتی، توسط یک سیستم کنترل تحت شبکه و هوشمند انجام می گیرد. این سیستم ها امکان مدی ری ت، هماهنگی و بهره برداری ای من، موثر و کارآمد از این واحدها را امکان پذیر می سازند. بزرگترین تهدید برای این سیستم ها، حملات هدف دار مانند حملات سایبری است که در آن مهاجم، راهبرد حمله خود را با هدف آسیب رساندن به سیستم تحت کنترل متناسب می کند. به منظور دستیابی به جامعه ای امن، توسعه زیرساخت های حفاظت شده، امن سازی اطلاعات حیاتی و تولید سیستم های کنترل مقاوم در برابر حملات سایبری بسیار حائز اهمیت است. راهبرد کلان بیشتر اسناد مهم و پرکاربرد در زمینه امنیت سیستم های کنترل صنعتی بر مبنای "راهبرد دفاع در عمق" استوار است. به منظور اجرای راهبرد کلان دفاع در عمق، راهکارهای گسترده ای پیشنهاد شده است. بنابراین، هدف این مقاله، بحث و توضیح این راهکارها در قالب دو دسته پایه ای ساختاری و با بررسی استانداردهای بین المللی و مقاله مروری بر منابع علمی و دانشگاهی ارائه شده در این زمینه از دید مهندسی کنترل و آشنایی متخصصین این حوزه با ضرورت و فرصت های پژوهش های مربوطه می باشد.

کلمات کلیدی:

حملات سایبری، تجهی زات صنعتی، آسیب پذیری، دفاع در عمق

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1463978>

