

آسیب شناسی روش های مواجهه با حملات سایبری

تالیف و تدوین

مسعود رفیعی

مریم طلایی

رسانا هدی زاده طاهری

ویراستار علمی

الهه یک کلام کاسانی

تنظیم و صفحه آرایی

کیمیا ابراهیمی

انتشارات: دانش گویا

عنوان: آسیب شناسی روش های مواجهه با حملات سایبری

موضوع: دسته بندی عوامل تاثیر گذار در صنعت نفت

واکاوی اکتشافات نفتی

مشخصات ظاهری: ص ۱۲۵

مشخصات نشر: دانش گویا

ISBN : 978 - 964 - 478-295 - 4

شابک: ۹۷۸-۹۶۴-۴۷۸-۲۹۵-۴

رده بستی: بزرگسال

شناسه مجوز: ۹-۳۵۰۱۵-۳۴۱۶۸۸

شمارگان: ۰۰۰ نسخه

نوبت چاپ: اول - بهار ۱۳۹۶

قیمت: ۴۵۰۰۰ تومان

مرکز پخش: Info_1998m@yahoo.com

☒ کلیه حق چاپ و نشر محفوظ و در انحصار سرپرست مولفین کتاب است و هرگونه استفاده از محتوای کتاب به داشتن اجازه ی کتبی از مولف نیازمند است این اثر مشمول "قانون حمایت از مولفان، مصنفان و هنرمندان" مصوب ۱۳۴۸/۱۱/۱۱ لذا بازنویسی، کپی برداری و تکثیر از روی تمام یا بخشی از آن در قالب تالیف، ترجمه، تلخیص، تست یا نرم افزار بدون اجازه کتبی مولف ممنوع بوده و متخلفین تحت پیگرد قانونی قرار خواهند گرفت. استفاده از مندرجات کتاب با ذکر منبع بلامانع است.

پیش گفتار

سیستم‌های صنعتی و نفتی به دور از چشم انسانها، عملیات کنترل و بهره برداری پلنت‌های نیروگاهها، پالایشگاه‌های نفت و گاز انجام می دهند. از آنجا که از گذشته حداکثر کارایی و سرعت در پروسه‌های کنترل صنعتی مطرح بوده، در نتیجه برای کاهش تاخیر در ارتباطات از پروتکل‌های بسیار ساده و فاقد مکانیسم امنیتی در شبکه‌های نفتی استفاده شده است. اما با پیشرفت روز افزون تکنولوژی و ورود سیستمهای فناوری اطلاعات به این سیستم‌ها به منظور تبادل اطلاعات، و ضعف امنیتی پروتکل‌های صنعتی، در نتیجه بسیاری از ریسکها و آسیب پذیری های دنیای اینترنت وارد سیستم‌های صنعتی شده است و این سیستم‌ها با چالش های امنیتی جدی با انجام حملات سایبری مواجه شده اند. در این تحقیق تلاش شده تا در ابتدا ریسک های حملات سایبری مربوط به سیستم های کنترل صنعتی را شرح داده و سپس راهکارهای موجود جهت امن سازی زیر ساختهای حیاتی کشور مانند نفت و گاز را در برابر حملات سایبری معرفی نماییم.

سربلند و پیروز باشید

فهرست مطالب

عناوین	صفحه
فصل اول.....	۱۱
۱-۱- مقدمه :.....	۱۲
۱-۲- آشنایی با حملات سایبری.....	۱۳
۱-۳- رورت شناخت حملات سایبری.....	۱۶
فصل دوم.....	۱۷
۲-۱- مقدمه :.....	۱۸
۲-۲- مفهوم جنگ سایبری.....	۱۹
۲-۳- حملات شناخته شده علیه اسکادا.....	۲۴
۲-۴- پیشروی امنیت در مواجهه با حملات سایبری.....	۲۸
۲-۵- شناخت و ارزیابی تهدیدات بالقوه.....	۳۲
۲-۶- نقاط آسیب‌پذیر سیستم کنترل صنعت.....	۳۲
۲-۷- روش‌های حمله به سیستم.....	۳۳
۲-۸- سیستم اسکادا چیست.....	۳۴
۲-۹- امنیت در سیستمهای کنترل صنعتی و زیرساختهای نفت.....	۳۵
۲-۱۰- پیشینه تحقیقات سیستم های اسکادا:.....	۳۶
۲-۱۱- برخی از روشهای مقابله با ddos.....	۴۰
فصل سوم.....	۴۲
۳-۱- مقدمه:.....	۴۳
۳-۲- سیستم اسکادا:.....	۴۷

- ۳-۳- اصول اساسی در سیستمهای اسکادا پیشرفته: ۴۷
- ۳-۴- حملات سایبری: ۴۹
- ۳-۵- مختصری از تاریخچه حملات سایبری در ایران ۵۸
- ۳-۶- ریسکها و حملات سایبری و عوامل تاثیرگذار آنها بر زیرساخت های نفت و گاز: ۶۰
- ۳-۷- انواع حملات در حین کار سیستم ها و روش مقابله با آنها: ۶۲
- ۳-۷-۱- حمله سایبری انکار سرویس (DOS و DDOS) ۶۲
- ۳-۷-۱-۲- دسته بندی حملات DDoS ۶۳
- ۳-۷-۱-۲- حملات پویش U2R : ۷۳
- ۳-۷-۳- حمله سایبری مردمیانی (MITM) : ۷۳
- ۳-۷-۴- اسب تروا، کرم ها، ویروس ها و کدهای خرابکار: ۷۴
- ۳-۷-۵- حمله سایبری کلاه عبور پیش فرض: ۷۶
- ۳-۷-۶- حملات شبکه بیسیم: ۷۷
- ۳-۷-۷- حملات Pishing : ۷۷
- ۳-۸- راهکارهای کاهش ریسک و جلوگیری از حملات سایبری در سیستم های نفتی ۸۱
- ۳-۹- روش های پیشگیری از حملات سایبری: ۹۱
- ۳-۱۰- روش های احراز هویت و پیشگیری از نفوذ در شبکه ها ۹۳
- ۳-۱۰-۱- امضا الکترونیک: ۹۳
- ۳-۱۰-۲- رمزهای عبور ۹۵
- ۳-۱۰-۳- استفاده از RSA: ۹۶
- ۳-۱۰-۴- سیستم های بايومتریک ۹۷
- ۳-۱۰-۵- رمز عبور یک بار ورود ۱۰۰

۱۰۳.....	۳-۱۰-۶- معرفی پروتکل Kerberos
۱۰۵.....	۳-۱۰-۷- پروتکل SESAME
۱۰۵.....	۳-۱۰-۸- پروتکل Kryptonite
۱۰۶.....	۳-۱۰-۹- معرفی port-knocking
۱۱۱.....	۳-۱۱- مزایا و معایب استفاده از pkn
۱۱۶.....	فصل چهارم
۱۱۷.....	۱-۱- مقدمه:
۱۱۷.....	۴-۲- بررسی دستیابی به اهداف پژوهش
۱۱۹.....	۵-۵- پیشنهادها، نظریات و پژوهشی
۱۲۰.....	۵-۶- تحلیل پایانی
۱۲۱.....	منابع