آگاهی وضعیتی سایبری

تألیف:

علی‌جبار رشیدی

کوروش داداش‌تبار احمدی

بهزاد نظرپور

سرشناسه: رشیدی، علی‌جبار، ۱۳۴۹- .
عنوان و نام پدیدآور: آگاهی وضعیتی سایبری/ تألیف علی‌جبار رشیدی، کوروش داداش‌تباراحمدی، بهزاد نظرپور.
مشخصات نشر: تهران: دانشگاه صنعتی مالک اشتر، ۱۳۹۶
مشخصات ظاهری: م، ۳۷۱ ص.: مصور(رنگی)، جدول، نمودار(بخشی رنگی).
شابک: ۰-۲۱-۷۷۳۶-۶۰۰-۹۷۸
وضعیت فهرست‌نویسی: فیپا.
یادداشت: واژه‌نامه.
یادداشت: کتابنامه: ص. [۳۲۸]-۳۵۰
موضوع: تروریسم رایانه‌ای- پیشگیری.
موضوع: جنگ اطلاعاتی
موضوع: فضای مجازی- تدابیر ایمنی.
شناسه افزوده: داداش‌تباراحمدی، کوروش، ۱۳۵۵- .
شناسه افزوده: نظرپور، بهزاد، ۱۳۶۰- .
شناسه افزوده: دانشگاه صنعتی مالک اشتر. انتشارات.
رده‌بندی کنگره: ۱۳۹۶ ۵ف۴ت/ ۶۷۷۳/۱۵ HV
رده‌بندی دیویی: ۳۶۳/۳۱
کتابشناسی ملی: ۴۹۷۶۵۳۴

دانشگاه صنعتی مالک اشتر

مجتمع دانشگاهی فناوری اطلاعات، ارتباطات و امنیت

عنوان کتاب: آگاهی وضعیتی سایبری
تألیف: علی‌جبار رشیدی- کوروش داداش‌تباراحمدی- بهزاد نظرپور
ناشر: انتشارات دانشگاه صنعتی مالک اشتر
طرح روی جلد: فریناز عسگری
لیتوگرافی، چاپ و صحافی: دانشگاه صنعتی مالک اشتر
صفحه‌آرایی رایانه‌ای: امین پژوهش
ویراستار ادبی: امین پژوهش
شمارگان: ۱۰۰۰ جلد
نوبت چاپ: اول، پاییز ۹۶
قیمت: ۲۷۰.۰۰۰ ریال

ISBN: 978-600-7736-21-0

آدرس: تهران، لویزان، دانشگاه صنعتی مالک اشتر، معاونت پژوهش و فناوری، مدیریت دانش، انتشارات. تلفن: ۲۲۹۳۲۸۹۱

پیشگفتار

افزایش بی سابقه حملات سایبری به شبکه‌های سازمانی و افزایش پیچیدگی این حملات سبب شده تا انگیزه پژوهش در زمینه آگاهی وضعیت سایبری روز به روز گسترش یابد. پژوهش‌هایی که تاکنون در این حوزه انجام گرفته بیش‌تر بر چگونگی درک راهبردهای چند مرحله‌ای و پیچیده حملات و هم‌چنین پیش‌بینی اقدامات آینده حمله متمرکز برده است. هر چند این تلاش‌ها، ایده‌هایی نویدبخش و جدید برای حوزه آگاهی وضعیتی سایبری به همراه داشته است اما ارزیابی میزان اثربخشی آن‌ها مغفول مانده است. نبود فرآیندهای مناسب، داده‌های استاندارد و قابل رجوع برای ارزیابی ابزارهای آگاهی وضعیتی سایبری، نیز یکی دیگر از مشکلات این حوزه است که آن هم بی‌دلیل نیست؛ چرا که تولید مجموعه داده‌ای واقعی که بتواند حملات چند مرحله‌ای روی پیکربندی‌های متنوع و بزرگ شبکه به همراه طیف کامل مهارت‌های نفوذ و حمله را فراهم نماید کار بسیار پرهزینه و زمان‌بری است.

هدف اصلی این کتاب که بر مبنای مطالعات و پژوهش‌های چندساله نویسندگان آن نگارش شده است ارائه، تحلیل، نقد و تدوین اطلاعات و دانش فنی و کاربردی در زمینه آگاهی وضعیتی سایبری است؛ به گونه‌ای که بتوان از این دانش به شکل موثری در سطوح مختلف از جمله آموزش در مقاطع تحصیلات تکمیلی و پژوهش استفاده نمود.

در این کتاب مفاهیم، نظریه‌ها، مدل‌ها، معماری‌ها و کاربردهای آگاهی وضعیتی سایبری و تجربیات موجود در این زمینه مورد مطالعه و بررسی قرار می گیرد که ساختار محتوایی فصل‌ها و بخش‌های آن به‌طور خلاصه در ادامه آمده است.

در **فصل اول**، اهمیت فضای سایبر و تعاریف مربوط به آگاهی وضعیتی در این فضا مورد بحث قرار گرفته، و در ادامه مدل‌های مربوط به آگاهی وضعیتی سایبری به همراه الزامات و چالش‌های پیش‌رو در زمینه سامانه‌های آگاهی وضعیتی سایبری مورد بررسی قرار می‌گیرند. در نهایت معیارهای ارزیابی کارآیی در سامانه‌های مذکور تشریح می‌شوند. در **فصل دوم**، مفاهیم و تعاریف کلی مقوله آگاهی وضعیتی تبیین شده و انواع مدل‌های ادغام اطلاعات که در سامانه‌های آگاهی وضعیتی کاربرد دارند، به همراه آگاهی وضعیتی سایبری مبتنی بر ادغام اطلاعات چندحسگری به‌طور مفصل تشریح می‌شوند.

در **فصل سوم**، فرآیند درک و فهم حملات سایبری که نقش بسزایی در سامانه‌های آگاهی وضعیتی سایبری ایفا می‌کند، در قالب فرآیندهای همبسته‌سازی هشدار و تولید سناریوهای حملات مورد بحث قرار گرفته و مفاهیم نوظهوری نظیر موتور ادغام اطلاعات در ردگیری حملات سایبری و مبانی هوشمندسازی این موتورها مورد تحلیل قرار می‌گیرد. در **فصل چهارم**، مقوله حس و پیش‌بینی حملات سایبری بر اساس مولفه‌هایی نظیر قابلیت، فرصت و نیت مهاجم مورد مطالعه قرار می‌گیرد و نحوه تجسم حملات سایبری مبتنی بر ادغام اطلاعات سطح بالا و همچنین پیش‌بینی حملات سایبری بر اساس یادگیری الگوها و رفتارهای حمله با استفاده از رویکردهایی نظیر مدل مارکوف تشریح می‌شود. در ادامه مفاهیمی نظیر مبهم‌سازی و تاثیر آن بر مدل‌سازی حملات سایبری و دادگان مورد نیاز برای استفاده در آگاهی وضعیتی سایبری پیشگویانه مورد بررسی قرار می‌گیرد. در **فصل پنجم**، سامانه‌های تعاملی نظیر صحنه نبرد سایبری، شبیه‌ساز و مصورساز حملات سایبری وهمچنین نقش و ارتباط آن‌ها در یک سامانه جامع آگاهی وضعیتی سایبری مورد مطالعه و بررسی قرار می‌گیرد.

با این توصیف کتاب حاضر، افزون بر این که بخشی از نیازهای پژوهش‌گران این شاخه علمی را برطرف می‌نماید، می‌تواند به عنوان مرجعی برای دوره‌های مختلف تحصیلی محسوب شود.

هر چند نویسندگان اهتمام زیادی در نگارش این کتاب داشته اند، با این حال از پیشنهادها و اصلاحاتی که پژوهشگران و خوانندگان کتاب ارائه نمایند استقبال کرده و در ویراستهای آینده از آن استفاده خواهد شد.

علی جبار رشیدی، کوروش داداش‌تبار احمدی، بهزاد نظرپور

فهرست مطالب