

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

راهنمای امنیت سایبری

تالیف:
فیدل هولتز

ترجمه:
ساسان کرمی زاده
شهرز ستوده

آراده کتاب

سرشناسه	: فیدل هولتز، گلن
عنوان و پدیدآور	: راهنمای امنیت سایبری / تالیف فیدل هولتز، ترجمه ساسان کرمی زاده، شهروز ستوده.
مشخصات نشر	: تهران، آراد کتاب، ۱۴۰۱
مشخصات ظاهری	: ۱۲۴ ص، مصور.
شابک	: ۹۷۸-۶۰۰-۱۸۶-۵۸۰-۰
یادداشت	: عنوان اصلی: {2021} The cyber security network guide
موضوع	: شبکه‌های کامپیوتری - تدابیر امنیتی
شناسه افزوده	: کرمی زاده، ساسان، ۱۳۶۳، مترجم
شناسه افزوده	: ستوده، شهروز، ۱۳۵۳، مترجم
رده بندی کنگره	: TK ۵۱۰۵ / ۵۹
رده بندی دیویی	: ۰۰۵ / ۸
شماره کتابخانه ملی	: ۸۹۲۳۷۰۵

راهنمای امنیت سایبری

☑ ترجمه: ساسان کرمی زاده، شهروز ستوده	☑ ناشر: آراد کتاب
☑ نوبت چاپ: اول	☑ سال چاپ: ۱۴۰۱
☑ تیراژ: ۱۰۰ جلد	☑ قیمت: ۱۲۵۰۰۰ تومان
شابک: ۹۷۸-۶۰۰-۱۸۶-۵۸۰-۰	

حق چاپ برای پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) با عنایت به قانون حمایت مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸ محفوظ است و متخلفین تحت پیگرد قانون قرار می گیرند.

مرکز پخش و فروش:

انتشارات آراد کتاب تلفن: ۰۶۶۹۷۵۲۸۵ - ۰۶۶۴۸۲۲۲۶ - ۰۹۳۵۳۰۶۲۴۵۸

فروشگاه اینترنتی: www.aradbook.com

پیشگفتار مؤلف

کتاب راهنمای شبکه سایبری، مطالعات در سیستم‌ها، تصمیم‌گیری و کنترل، چشم‌اندازی اساسی فنی امنیت سایبری از قابلیت‌های عملیاتی سایبری دولت بین‌المللی را برای دانشجویان مقطع کارشناسی و کارشناسی ارشد ارائه می‌کند؛ که شامل رویه‌های عملیاتی استاندارد، مستندات عملیات سایبری، و شرح ابزارهای مورد استفاده در رویداد یک حادثه سایبری بزرگ است.

هدف از این کتاب، مطالعات در سیستم‌ها، کنترل و تصمیم‌گیری، استانداردسازی الزامات برای تحلیلگران عملیاتی بین‌المللی فیزیکی سایبری و پاسخ‌دهی به شرکت‌کنندگان سایبری است.

این کتاب راهنمای فنی منحصربه‌فرد اطلاعات پس‌زمینه منبع باز مناسب را در اختیار تحلیلگران سایبری قرار می‌دهد تا تلاش‌ها را برای ارائه ورودی‌های دقیق و جامع در توسعه محصولات تحلیلی سایبری تقویت کند.

پیشگامان سایبری تلاش می‌کنند اطلاعات مهم سایبری را با همکاری دولت‌های بین‌المللی در مورد آسیب‌پذیری و تجزیه و تحلیل پیامدها برای پاسخ به حملات شبکه‌های سایبری ارائه دهند.

فیدل هولتز

فهرست مطالب

عنوان	صفحه
پیشگفتار مؤلف	5
فصل 1: تجزیه و تحلیل و برنامه‌ریزی پیش از وقوع حادثه	9
1.1 نظارت مداوم و پایا	9
فصل 2: شناسایی و تشخیص رویداد	11
2.1 تشخیص	12
2.2 تحلیل تهدید	15
2.3 تجزیه و تحلیل بدافزار	19
2.4 فرایند اطلاع‌رسانی تهدیدات سایبری	20
فصل 3: آسیب‌پذیری / تجزیه و تحلیل پیامد	23
3.1 به اشتراک‌گذاری اطلاعات	23
3.2 تجزیه و تحلیل پیامد/آسیب‌پذیری	23
3.2.1 جمع‌آوری داده‌های سایبری	25
3.2.2 تجزیه و تحلیل فیزیکی سیستم‌های وابسته/کنترل شده سایبری	26
3.3 تجزیه و تحلیل وابستگی/وابستگی متقابل	36
3.3.1 شناسایی تأثیرات داخلی	37
3.3.2 شناسایی تأثیرات خارجی	39
3.4 گزارش تجزیه و تحلیل	41
فصل 4: جبران و پاسخ به رویداد	47
4.1 به اشتراک‌گذاری اطلاعات	47
4.1.1 پاسخ به رویداد سایبری	47
4.1.2 آگاه‌سازی مقامات مراکز عملیاتی سایبری	48
4.1.3 بررسی و ارائه بازخورد از مرکز عملیات سایبری	48
4.1.4 هماهنگی به منظور تحلیل فیزیکی سایبری	48
4.1.5 انجام تحلیل و به اشتراک‌گذاری تحلیل	48
4.1.6 آگاهی موقعیتی	48
4.2 فعالیت‌های کاهش میزان اثر	49
4.2.1 شناسایی و بررسی پیکربندی سیستم فیزیکی	49

49	4.2.2 بازسازی سیستم‌ها.....
49	4.2.3 تدوین و اجرای فرآیند
50	4.3 پاسخ و بازسازی
50	4.3.1 تشریح مقاومت زیرساخت‌های مورد نظر برای تعیین برنامه‌های پاسخ و بازسازی
51	4.3.2 شناسایی محدودیت‌ها و یا محدودیت‌های برنامه اجرایی پاسخ و بازسازی
51	4.3.3 چارچوب زمانی پروژه برای برنامه پاسخ و بازسازی
51	4.3.4 پیامدهای محلی، ایالتی، منطقه ای و ملی
52	4.3.5 احتمال و پیامد کیفی/کمی پاسخ رویداد اختلال
53	4.3.6 توزیع پیامد
53	4.4 تجزیه و تحلیل رسانه‌های دیجیتال سایبری و فیزیکی
55	فصل 5: معماری ابری
55	5.1 مدل‌های سرویس ابری
56	5.2 مدل‌های استقرار
57	5.3 مدل‌های ابری خدمات وب آمازون
57	5.4 مدل‌های ابری خدمات وب آژور
59	فصل 6: درس‌های آموخته شده
61	پیوست A: (SOP) رویه عملیاتی سخت‌افزار و نرم‌افزارهای شبکه سایبری
66	پیوست B: پروسه آنالیز ماتریس چهارچوب مسیر دهی (نگاشت) فیزیکی - سایبری
67	پیوست C: ده حمله برتر سایبری OWASP
71	پیوست D: اصطلاحات در مورد اطلاعات تهدید ساختاریافته (STIX™)
79	پیوست E: مدل مرجع اتصالات (ارتباطات داخلی) سیستم‌های باز
90	پیوست F: ابزارهای امنیت سایبری
93	پیوست G: سرنام‌ها و اختصارات
100	پیوست H: واژه نامه اصطلاحات
120	منابع