

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

کاستن تهدیدات فراگیر امنیت سایبر

رشته: پیتر سامر، یان براون

مترجم: سید علی قلی زاده



سرشناسه	سامر، پيتر :
عنوان و نام پديدآور	کاستن تهديدات فراگير امنيت سايبر / نوشته پيتر سامر، يان براون؛ مترجم زين العابدين قلي زاده.
مشخصات نشر	تهران : نيروي انتظامي جمهوري اسلامي ايران، پليس فتا، ۱۳۹۲.
مشخصات ظاهري	۱۲۹ ص. مصور (بخشي رنگي).
شابک	۹-۴-۹۳۴۰۱-۶۰۰-۹۷۸
وضعيت فهرست نويي	فيا :
يادداشت	کتاب حاضر ترجمه کتاب الكترونيكي تحت عنوان Reducing systemic cybersecurity risk, 2011 است.
يادداشت	کتابنامه: ص. ۱۳۹.
موضوع	شبکه‌های کامپيوتری - تدابير ايمني
موضوع	کامپيوترها - ايمني اطلاعات
موضوع	فضای مجازی - تدابير ايمني
موضوع	جنگ اطلاعاتي
شناسه افزوده	براون، يان
شناسه افزوده	Brown, Ian
شناسه افزوده	قلي زاده، زين العابدين، ۱۳۶۳ -، مترجم
شناسه افزوده	نيروي انتظامي جمهوري اسلامي ايران، پليس فتا
رده‌بندی کنگره	۱۳۹ ک ۲۳ / ۵۹ / ۵۱۰۵ TK
رده بندی ديويي	۸ / ۵
شماره کتابشناسي ملي	۷۵۲



نام کتاب	کاستن تهديدات فراگير امنيت :
ناشر	پليس فتا :
مولفان	پيتر سامر، يان براون :
مترجم	زين العابدين قلي زاده :
نظارت	محسن خداپرست :
چاپ اول	۱۳۹۲ :
تيراژ	۱۰۰۰ جلد :
ليتوگرافي، چاپ و صحافي	چاپ و نشر حديث کوثر :
قيمت	۵۰۰۰۰ ريال :
شابک	۹-۴-۹۳۴۰۱-۶۰۰-۹۷۸ :
ISBN	978-600-93401-4-9 :

فهرست مطالب

فصل اول: خلاصه اجرایی	۷
فصل دوم: خطرات سیستمی در امنیت سایبری	۱۳
تألیف	۱۷
فصل سوم: تعریف زمینه‌ی تاریخی	۲۱
روزهای آژینت و رایانش دولتی	۲۱
دهه‌ی ۱۹۷۰ و ۱۹۸۰: انگیزه‌ی متغیر خطر	۲۲
مسیرهای برق‌رایی دموکراسی	۲۳
ظهور اینترنت	۲۴
توسعه‌ی اینترنت در آینده	۲۶
تغییر در کسب‌وکار	۲۷
دولت الکترونیک	۲۸
شبکه‌های توری هوشمند و اسکادا	۲۹
رایانش ابری	۲۹
پیچیدگی / خطوطِ مبدا / کُند / کاستی‌های برنامه	۳۰
زیرساخت‌های بحرانی: عناصر سایبری	۳۱
تهدیدهای سیستمیک خاص	۳۲
حملات فیزیکیِ عمدی	۳۸
حملات ترکیبی	۴۲

۴۳	حملات تبهکارانه‌ی گسترده
۴۵	هک از روی سرگرمی
۴۵	هک گرایی
۴۷	جاسوسی صنعتی و دولتی در مقیاس گسترده
۵۱	فصل چهارم: راه‌حل‌ها
۵۱	راه‌حل‌ها: بهترین‌های امنیت
۵۳	راه‌حل‌ها: طراحی سیستم‌نیازمندی‌های سیستمیک / طراحی / امنیتی
۵۳	سیستم‌های بی‌خطر
۵۴	راه‌حل‌ها: اقدامات امنیتی و تشخیصی فناوری‌های امنیتی / اختصاصی
۵۸	راه‌حل‌ها: کاستن از تأثیرات و بازسازی
۶۰	توصیف خطر، اینترلینک‌ها (Interlinkages) و تأثیرات جانبی
۶۷	مشکلات برنامه‌ریزی یک جنگ سایبری
۶۸	تحلیل خطر (Risk Analysis) و زمینه وسیع‌تر تأثیر، دانه و استمرار
۶۸	آستانه، tipping و نقاط کنترل
۷۰	چالش‌های مربوط با زمان
۷۱	اشخاص
۷۲	تجارت
۷۴	خدمات دولتی
۷۶	زیرساخت حیاتی ملی
۷۶	کلاهبرداری
۷۷	جاسوسی علیه دولت‌ها، کسب‌وکارها و سازمان‌های غیردولتی

۷۸	حمله جهت از دسترس خارج کردن زیرساخت‌های حیاتی
۸۱	بدافزارها و تهدیدهای جهانی
۸۵	فصل پنجم: سطح آمادگی
۸۵	واکنش‌های نظامی
۸۸	انطباقات غیرنظامی
۹۰	بخش خصوصی
۹۲	دولت، بخش خصوصی و مشارکت بخش‌های دولتی و خصوصی
۹۴	پلیس و مقابله با کلاهبرداری
۹۶	کارهای پژوهشی
۹۷	راهنماهای حقوقی و قانونی
۹۸	معاهده جرایم سایبری شورای اروپا
۹۹	سازمان ملل متحد
۹۹	شورای اروپا
۱۰۰	سازمان کشورهای آمریکایی
۱۰۰	سازمان توسعه و همکاری‌های اقتصادی
۱۰۱	رویکردهای ملی
۱۰۱	قوانین بین‌المللی و همکاری بخش خصوصی
۱۰۵	نقش فناوری در مقابله با شرایط اضطراری
۱۱۱	فصل ششم: نتیجه‌گیری و پیشنهادها
۱۱۳	راهنماهای ملی
۱۱۴	واکنش‌های نظامی

- ۱۱۵ اثرات غیرنظامی
- ۱۱۵ همکاری بخش خصوصی و دولتی
- ۱۱۶ راهبردهای بین‌المللی
- ۱۱۷ اقدامات ممکن جدید در زمینه فنی
- ۱۱۸ پژوهش
- ۱۱۹ آموزش
- ۱۲۱ فهرست منابع