

مدیریت خطرهای سایبری

نویسنده

پیام حجازیان

www.ketab.ir

دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

مرکز انتشارات راهبردی

تهران - ۱۳۹۸

سیرشناسه	حجازیان، پیام، ۱۳۷۲ -
عنوان و نام پدیدآور	مدیریت خطرهای سایبری/ نویسنده پیام حجازیان.
مشخصات نشر	تهران: دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، مرکز انتشارات راهبردی، ۱۳۹۸.
مشخصات ظاهری	۲۷۸ ص.
شابک	۹۷۸-۶۲۲-۲۴۸-۰۳۰-۱:
وضعیت فهرست نویسی	فیا
موضوع	جرایم کامپیوتری -- پیشگیری
موضوع	Computer crimes -- Prevention
موضوع	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	Computer networks -- Security measures
شناسه افزوده	دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی. انتشارات
رده بندی کنگره	HV۶۷۷۳
رده بندی دیویی	۰۰۵/۸
شماره کتابشناسی ملی	۵۸۱۸۰۵



مدیریت خطرهای سایبری

تألیف: پیام حجازیان

ویراستار ادبی: مهدی یوسفی

ناظر ویراستاری: مهران غلامیان

صفحه آرا: علی مهدی زاده

طراح جلد: زهرا مهدوی

نوبت چاپ: اول - ۱۳۹۸

ناشر: انتشارات دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

شمارگان: ۱۰۰۰ نسخه

قیمت: ۵۲۰۰۰۰ ریال

همه حقوق چاپ و نشر این کتاب محفوظ است.

انتشارات دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

نشانی انتشارات: تهران، ضلع شمالی بزرگراه شهید بابایی، بعد از اتوبان هنگام،

دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، انتشارات دانشگاه عالی دفاع ملی

نشانی اینترنتی: www.sndu.ac.ir

تلفن: ۲۲۹۷۰۳۴۳

فهرست مطالب

۲۱	فصل اول: مقدمه
۲۴	۱-۱- هدف و تأکید
۲۵	۱-۲- سیاست تحریر و ارائه‌ی آن
۲۶	۱-۳- ساختار و سازمان
۲۶	۱-۳-۱- بخش ۱: مقدمه‌ای مفهومی
۲۷	۱-۳-۲- بخش ۲: نمونه‌ای از ارزیابی خطر سایبری
۲۸	۱-۳-۳- بخش سوم: چالش‌های شناخته‌شده
۳۰	۱-۴- خوانندگان پیشنهادی راه‌های خواندن
۳۱	۱-۵- استانداردهای بوطه
۳۵	قسمت اول: مقدمه‌ای مفهومی
۳۷	فصل دوم: مدیریت خطر
۳۹	۱-۲- خطر چیست
۴۳	۲-۲- مدیریت خطر چیست
۴۵	۲-۳- ارتباطات و مشاوره
۴۶	۱-۳-۲- ایجاد یک گروه مشورتی
۴۶	۲-۳-۲- تعریف یک طرح برای ارتباط و مشاوره
۴۷	۲-۳-۳- اطمینان از تأیید فرآیند مدیریت خطر
۴۷	۲-۳-۴- ارتباط با نتایج ارزیابی خطر
۴۸	۲-۴- ارزیابی خطر
۴۸	۱-۴-۲- ایجاد زمینه
۵۲	۲-۴-۲- شناسایی خطر
۵۵	۲-۴-۳- تحلیل خطر
۵۷	۲-۴-۴- ارزیابی خطر
۵۸	۲-۴-۵- طرز عمل خطر
۵۹	۲-۵- نظارت و بررسی
۶۰	۱-۵-۲- نظارت و بررسی خطر
۶۰	۲-۵-۲- نظارت و بررسی مدیریت خطر

۶- ۲- مطالب اضافی برای خواندن..... ۶۱

فصل سوم: سیستم‌های سایبری..... ۶۳

۱- ۳- فضای مجازی چیست..... ۶۵

۲- ۳- سیستم سایبری چیست..... ۶۶

۳- ۳- مطالب اضافی برای خواندن..... ۶۷

فصل چهارم: امنیت سایبری..... ۷۱

۱- ۴- امنیت سایبری چیست..... ۷۳

۲- ۴- چگونه امنیت سایبری به امنیت اطلاعات مربوط است..... ۷۴

۳- ۴- چگونه امنیت سایبری به حفاظت زیرساخت‌های بحرانی مرتبط است..... ۷۵

۴- ۴- چگونه امنیت سایبری به حفاظت زیرساخت‌های بحرانی است..... ۷۶

۵- ۴- مطالب اضافی برای خواندن..... ۷۷

فصل پنجم: مدیریت خطر سایبری..... ۷۹

۱- ۵- خطر سایبری چیست..... ۸۱

۲- ۵- ارتباط و مشاوره در مورد خطر سایبری..... ۸۳

۳- ۵- ارزیابی خطر سایبری..... ۸۴

۱- ۳- ۵- ایجاد زمینه برای خطر سایبری..... ۸۶

۲- ۳- ۵- شناسایی خطر مخرب سایبری..... ۸۷

۳- ۳- ۵- شناسایی خطر ابتلا به سایبری غیر مخرب..... ۹۱

۴- ۳- ۵- تحلیل خطر سایبری..... ۹۵

۵- ۳- ۵- ارزیابی خطر سایبری..... ۹۷

۶- ۳- ۵- طرز عملی برای خطر سایبری..... ۹۸

۴- ۵- نظارت و بررسی خطر سایبری..... ۱۰۰

۱- ۴- ۵- نظارت و بررسی خطر ابتلا به سایبر..... ۱۰۰

۲- ۴- ۵- نظارت و بررسی مدیریت خطر سایبری..... ۱۰۱

۵- ۵- مطالب اضافی برای خواندن..... ۱۰۲

قسمت دوم: ارزیابی خطر سایبری با نشان دادن مثال..... ۱۰۳

فصل ششم: ایجاد زمینه..... ۱۰۵

۱۰۷	۶-۱- زمین‌های اهداف
۱۰۸	۶-۱-۱- زمین‌های بیرونی
۱۰۸	۶-۱-۲- زمین‌های داخلی
۱۰۹	۶-۱-۳- اهداف
۱۰۹	۶-۲- اهداف ارزیابی
۱۱۰	۶-۲-۱- مشتری برق
۱۱۲	۶-۲-۲- اپراتور سیستم توزیع کننده
۱۱۲	۶-۲-۳- کانال‌های ارتباطی بین قطعات
۱۱۲	۶-۳- رابط به فضای مجازی و سطح حمله
۱۱۳	۶-۴- حوزه، تمرکز و مفاهیم
۱۱۴	۶-۴-۱- حوزه
۱۱۴	۶-۴-۲- تمرکز
۱۱۵	۶-۴-۳- مفاهیم
۱۱۵	۶-۵- دارایی، مقیاس، معیارهای ارزیابی خطر
۱۱۶	۶-۵-۱- دارایی
۱۱۶	۶-۵-۲- مقیاس احتمال
۱۱۷	۶-۵-۳- مقیاس‌های پیامد
۱۱۹	۶-۵-۴- معیارهای ارزیابی خطر
۱۲۰	۶-۶- مطالب اضافی برای خواندن
۱۲۱	فصل هفتم: شناسایی خطر
۱۲۳	۷-۱- روش‌های شناسایی خطر
۱۲۹	۷-۲- خطرات مضر
۱۳۰	۷-۲-۱- شناسایی منبع تهدید
۱۳۲	۷-۲-۲- تشخیص تهدید
۱۳۶	۷-۲-۳- شناسایی آسیب‌پذیری
۱۳۹	۷-۲-۴- شناسایی حوادث
۱۴۵	۷-۳- خطرات مخرب
۱۴۷	۷-۳-۱- شناسایی حوادث
۱۵۰	۷-۳-۲- شناسایی آسیب‌پذیری
۱۵۲	۷-۳-۳- تشخیص تهدید
۱۵۴	۷-۳-۴- شناسایی منبع خطر
۱۵۶	۷-۴- مطالب اضافی برای خواندن

فصل هشتم: تحلیل خطر..... ۱۵۹

- ۱۶۲..... ۸-۱- تحلیل تهدید.....
- ۱۶۳..... ۸-۱-۱- تهدیدات مخرب.....
- ۱۶۵..... ۸-۱-۲- تهدیدات غیر مخرب.....
- ۱۶۷..... ۸-۲- تجزیه و تحلیل آسیب پذیری.....
- ۱۶۷..... ۸-۲-۱- آسیب پذیری های تهدیدات مخرب.....
- ۱۶۸..... ۸-۲-۲- آسیب پذیری های حاصل از تهدید غیر مخرب.....
- ۱۶۹..... ۸-۳- احوال حوادث.....
- ۱۷۱..... ۸-۴- پیامدهای حوادث.....
- ۱۷۲..... ۸-۵- مطالب اضافی برای خواندن.....

فصل نهم: ارزیابی خطر..... ۱۷۵

- ۱۷۷..... ۹-۱- تثبیت نتایج تحلیل و تحلیل خطر.....
- ۱۷۸..... ۹-۲- ارزیابی سطح خطر.....
- ۱۷۹..... ۹-۳- جمع آوری خطر.....
- ۱۸۵..... ۹-۴- گروه بندی خطر.....
- ۱۸۶..... ۹-۵- مطالب اضافی برای خواندن.....

فصل دهم: طرز عمل خطر..... ۱۸۷

- ۱۸۹..... ۱۰-۱- شناسایی طرز عمل خطر.....
- ۱۸۹..... ۱۰-۱-۱- خطرات مخرب.....
- ۱۹۲..... ۱۰-۱-۲- خطرات غیر مخرب.....
- ۱۹۶..... ۱۰-۲- پذیرش خطر.....
- ۱۹۹..... ۱۰-۳- مطالب اضافی برای خواندن.....

قسمت سوم: چالش های شناخته شده و راه های مقابله با آن در عمل..... ۲۰۱

فصل یازدهم: کدام یک از روش های اندازه گیری سطح خطر استفاده می شوند..... ۲۰۳

- ۲۰۵..... ۱۱-۱- اندازه گیری دو عامله.....
- ۲۰۶..... ۱۱-۲- اندازه گیری سه عامله.....
- ۲۰۷..... ۱۱-۳- اندازه گیری چند عامله.....
- ۲۰۹..... ۱۱-۴- کدام روش اندازه گیری برای خطر سایبری مورد استفاده قرار می گیرد.....
- ۲۱۰..... ۱۱-۵- مطالب اضافی برای خواندن.....

۲۱۱	فصل دوازدهم: چه مقیاسی تحت چه شرایطی مناسب است
۲۱۳	۱ - ۱۲ - طبقه‌بندی مقیاس‌ها
۲۱۵	۲ - ۱۲ - ارزیابی خطر کیفی در مقابل کمی
۲۱۷	۳ - ۱۲ - مقیاسهایی برای احتمال
۲۱۹	۴ - ۱۲ - مقیاس برای نتیجه
۲۲۰	۵ - ۱۲ - چه مقیاس‌هایی برای خطر سایبر استفاده می‌شود
۲۲۱	۶ - ۱۲ - مطالب اضافی برای خواندن
۲۲۳	فصل سیزدهم: چگونه با تردید مواجه شویم
۲۲۵	۱ - ۱۳ - تعریف مفهومی
۲۲۶	۲ - ۱۳ - انواع تردید
۲۲۸	۳ - ۱۳ - نمایش تردید
۲۳۰	۴ - ۱۳ - کاهش تردید
۲۳۱	۵ - ۱۳ - چگونه تردید ایمن‌سازی را مدیریت کنیم
۲۳۲	۶ - ۱۳ - مطالب اضافی برای خواندن
۲۳۳	فصل چهاردهم: خطری با پیامد بالا، احتمال کم
۲۳۵	۱ - ۱۴ - نحوه‌ی برخورد با قوهای سیاه
۲۳۷	۲ - ۱۴ - شناسایی قوهای خاکستری
۲۳۸	۳ - ۱۴ - برقراری ارتباط با قوهای خاکستری
۲۳۹	۴ - ۱۴ - نحوه‌ی برخورد با قوهای خاکستری
۲۳۹	۵ - ۱۴ - شناختن قوهای خاکستری در فضای مجازی
۲۴۰	۶ - ۱۴ - مطالب اضافی برای خواندن
۲۴۱	فصل پانزدهم: نتیجه‌گیری
۲۴۳	۱ - ۱۵ - آنچه ما به‌طور کلی در پیش گرفته‌ایم
۲۴۵	۲ - ۱۵ - آنچه ما به‌ویژه به آن اشاره کردیم
۲۴۶	۳ - ۱۵ - آنچه را که ما پوشش نداده‌ایم
۲۵۱	مراجع
۲۶۱	نمایه
۲۷۵	اختصارات

فناوری اطلاعات و ارتباطات^۱ بیش از چندین دهه مزایای قابل توجهی برای شرکت‌ها، افراد و جامعه به ارمغان آورده است. با توجه به تأثیر گسترده و عمیق اینترنت در بسیاری از بخش‌های زندگی روزمره‌ی ما، این موضوع وضوح مشهود است. اینترنت و به‌طور گسترده‌ای فضای مجازی، سنگ بنای طیف وسیعی از خدمات و فعالیت‌هایی هستند که امروزه با آن‌ها سروکار داریم. با توجه به فضای مجازی و زیرساخت‌های آن، افراد و سازمان‌ها به خدمات بش‌تر و بهتر از قبل دسترسی دارند. این مورد در حوزه‌های مختلف جامعه شامل بانکداری و مالی، ارتباطات، سرگرمی، بهداشت، تأمین برق، تعاملات اجتماعی، حمل و نقل، تجارت، مشارکت اجتماعی مشهود است. در نتیجه، زندگی روزانه ما، حقوق اساسی، اقتصاد، و امنیت اجتماعی بستگی به کارکرد فناوری اطلاعات و ارتباطات یکپارچه دارد. در عین حال، فضای مجازی نیز تهدیدات و آسیب‌پذیری‌های جدیدی را ارائه کرده است و همپایان^۲ معرفی این آسیب‌ها و تهدیدات ادامه می‌دهد. شرکت‌کنندگان در معرض حوادث سایبری در بسیاری از انواع و درجات سختی قرار دارند. این تهدیدات و خطرات شامل سرقت اطلاعات، اختلال در سرویس‌ها، سوءاستفاده از حریم شخصی و هویت، تقلب، جاسوسی و خرابکاری است. در مقیاس وسیع، نیز جوامع تحت تأثیر تهدید حملات احتمالی به زیرساخت‌های حیاتی از طریق فضای مجازی، و همچنین احتمال حملات تروریستی سایبری و حتی جنگ سایبری قرار دارند. علاوه بر بسیاری از امکانات جاسوسی سایبری و حملات مخرب، اتفاقات دیگری تهدیدات غیر مخرب ممکن است منجر به حوادث امنیتی سایبری شوند. در حقیقت، تعداد زیادی از خطراتی که ما به‌طور سنتی در دنیای فیزیکی در معرض آن قرار گرفته‌ایم، در فضای مجازی ظاهر می‌شوند و به خطر سایبری تبدیل شده‌اند. به‌منظور اطمینان از سطح رضایت‌بخش امنیت سایبری، ذینفعان باید ماهیت خطر سایبر را درک کنند و آنچه را که خطر سایبری را

از سایر انواع خطر متمایز می‌سازد تشخیص دهند، و به روش‌ها و فن‌های مناسب برای مدیریت خطرهای سایبری نیاز دارند. هدف اصلی ما از این کتاب این است که مقدمه‌ی کوتاهی در مورد مدیریت خطر، تمرکز بر امنیت سایبری و ارزیابی خطرهای سایبری ارائه دهیم. خواننده را با اصطلاحات اساسی آشناسازیم. ما در حال ارائه و توضیح فرآیندهای مدیریت خطرهای سایبری هستیم، و نمونه‌هایی از چگونگی انجام ارزیابی خطر سایبر در عمل را ارائه می‌دهیم. علاوه بر این، بسیاری از چالش‌های معمول را که مخاطبان ارزیابی خطر در نیاز می‌گیرند را مورد بررسی قرار می‌دهیم، و ما در مورد چگونگی مقابله با آن‌ها توصیه‌هایی ارائه می‌دهیم.

تکنیک‌ها، ابزارها، یا مدل‌های مدلسازی و قالب‌های مستندسازی مختلفی موجود است تا از بررسی خطر سایبری حمایت کند. این کتاب به هر رویکرد خاصی بی‌اعتنا است، در حالی که اساس این کتاب بر اساس استانداردهای موجود و بهترین شیوه‌های صنعتی بنا نهاده شده است، ما فرآیند بررسی خطر و مثال‌ها را در قالبی نشان می‌دهیم که بتوان با هر رویکرد خاصی که در تطابق با استاندارد مدیریت خطر ایزو ۳۱۰۰۰ است، معرفی شود. مخاطبان اصلی این کتاب متخصصان و اعضای انجمن‌های تخصصی فارغ التحصیلان حوزه‌ی فناوری اطلاعات و ارتباطات می‌باشند. همچنین هدف از تربیت اساتیدی با ابزار آموزشی مناسب پیرامون اصول، قواعد و فن‌های مدیریت خطر سایبری است. ما همچنین اعتقاد داریم که این کتاب بسیاری از جنبه‌ها و مفاهیم حوزه‌ی امنیت سایبری را روشن می‌سازد. از این رو این کتاب می‌تواند برای محققانی که در حوزه‌های مرتبط با امنیت سایبری فعالیت دارند مفید واقع گردد. دانش و تجربه‌ی ما پیرامون امنیت سایبری و مدیریت خطر سایبری و همچنین مطالب موجود در این کتاب عمدتاً برگرفته از تحقیقات علمی و مطالعات تجربی مشترک با همکاران صنعتی است. از تمام افرادی که به طرق مختلف ما را در نگارش این کتاب کمک کردند تشکر می‌کنیم. ما از همکاران نزدیک خود گنسر اردوگان^۱، یان لی^۲،

آیدا اومروویچ^۱ و فدریک سیهوسن^۲ برای نظرات و پیشنهادهای متعددشان در بسیاری از قسمت‌های این کتاب تشکر می‌کنیم. از کریستین بکرز^۳، کارین برنسمد^۴، آسلاک وگنر ایده^۵، ماریکا لودرز^۶ و راگنهیلد کوبرو رونده^۷ برای بازبینی این کتاب و تهیه‌ی بازخورد خوب و مفید سپاسگزاریم.

قبل و در حین کار بر روی این کتاب از همکاری افراد دانشگاهی و صنعتی در پروژه‌های تحقیقاتی متعدد بسیار سود برده‌ایم. این افراد عبارت‌اند از: یورگن گروومن^۸، ماریتا هیسل^۹، فابیو مارتینلی^{۱۰}، ولتر پیترز^{۱۱}، الکساندر پرتسکنر^{۱۲}، کریستین و. پروبست^{۱۳} و آریستوتلیست ژافالیاس^{۱۴}.

حمایت مالی برخی از فعالیت‌های تحقیقاتی مربوط به این کتاب توسط شورای پژوهشی نروژ^{۱۵} از طریق پروژه‌های الماس^{۱۶} و آگرا^{۱۷} انجام گرفته است. تأمین مالی فعالیت‌های تحقیقاتی مربوط به سلهی کمسیون اروپا^{۱۸}، به‌ویژه از طریق پروژه‌های راسن^{۱۹}، نسوس^{۲۰} و همچنین^{۲۱} صورت گرفته است.

نویسندگان: اتله رفسدال^{۲۲}، بچورنار سولهاگ^{۲۳}، کتیل استلن^{۲۴}

-
- 1 Aida Omerovic
 - 2 Fredrik Sechusen
 - 3 Kristian Beckers
 - 4 Karin Bernsmed
 - 5 Aslak Wegner Eide
 - 6 Marika Luders
 - 7 Ragnhild Kobro Runde
 - 8 Jürgen Großmann
 - 9 Maritta Heisel
 - 10 Fabio Martignoli
 - 11 Wolter Pieter
 - 12 Alexander Peterschneider
 - 13 Christian W. Probst
 - 14 Aristotelis Tzafalias
 - 15 Research Council of Norway
 - 16 Diamonds
 - 17 AGRA
 - 18 European Commission
 - 19 RASEN
 - 20 NESSOS
 - 21 CONCERTO
 - 22 Atle Refsdal
 - 23 Bjørnar Solhaug
 - 24 Ketil Stølen