بسم الله الرحمن الرحیم

راهبردهای امنیت سایبری

(جلد دوم)

شناسایی و فریب

گردآوری و تدوین
معاونت پژوهش و تولید علم

دانشگاه اطلاعات و امنیت ملی
مؤسسه چاپ و انتشارات
۱۳۹۶

عنوان و نام پدیدآور	: راهبردهای امنیت سایبری/ گردآوری و تدوین معاونت پژوهش و تولید علم، [دانشگاه اطلاعات و امنیت ملی].
مشخصات نشر	: تهران: دانشگاه اطلاعات و امنیت ملی، مؤسسه چاپ و انتشارات، ۱۳۹۶.
مشخصات ظاهری	: ۳ ج. ش. ۳۵۶.
شابک	: ۸ـ۸۸ـ۸۴۱۱ـ۶۰۰ـ۹۷۸؛ ۳۰۰۰۰۰ ریال
وضعیت فهرست‌نویسی	: فیپا
یادداشت	: ج. ۳ (چاپ اول: ۱۳۹۶) (فیپا).
یادداشت	: کتابنامه.
مندرجات	: ج. ۱. سیاست‌گذاری. – ج. ۲. شناسایی و فریب. – ج. ۳. حفاظت.
موضوع	: شبکه‌های کامپیوتری – تدابیر ایمنی
موضوع	: Computer networks – Security measures
موضوع	: اینترنت – تدابیر ایمنی
موضوع	: Internet – Security measures
شناسه افزوده	: دانشگاه اطلاعات و امنیت ملی. مؤسسه چاپ و انتشارات
شناسه افزوده	: دانشگاه اطلاعات و امنیت ملی. معاونت پژوهش و تولید علم
رده‌بندی کنگره	: ۱۳۹۶ ۲ر/۵۱۰/۵TK
رده‌بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۴۷۷۶۱۹۰

عنوان: راهبردهای امنیت سایبری (۱ جلد در ۳). شناسایی و فریب

گردآوری و تدوین: معاونت پژوهش تولید علم

ناشر: مؤسسه چاپ و انتشارات دانشگاه اطلاعات و امنیت ملی

تاریخ انتشار: ۱۳۹۶

نوبت چاپ: اول

بها: ۳۰۰۰۰۰ ریال

شابک: ۹۷۸ـ۶۰۰ـ۸۴۱۱ـ۸۸ـ۸

شمارگان: ۱۰۰۰نسخه

شماره تلفن: ۲۲۴۶۹۷۳۹

تهران: صندوق پستی ۱۴۳۸-۱۶۷۶۵

مقدمه ناشر

در فصل اول کتاب با عنوان «شناسایی و نظارت دیجیتال» ضمن ارائه اصول پایه‌ای نظارت، نظارت و دفاع سایبری ارائه، تاریخچه و کاربردهای عملی اصول مذکور و چگونگی ورود آنها به دنیای دیجیتال بررسی می‌گردد. در ادامه ضمن تشریح مبانی شناسایی و نظارت دیجیتال، با ارائه پیشینه‌ای از موضوع، زمینه برای فصول آینده که در آنها به تفصیل چگونگی انجام این فعالیت‌ها، میزان آسیب‌پذیری‌ها و چگونگی افزایش دفاع و کاهش خطر در سطح شخصی پرداخته می‌شود، مهیا می‌گردد.

فصل دوم به موضوع «جمع آوری اطلاعات» می‌پردازد و طی آن شیوه‌های جمع‌آوری اطلاعات برای توسعه اشرافیت بر یک هدف خاص در دنیای سایبری مورد بحث قرار می‌گیرد. رد پایی که هر کنشگر سایبری در دنیای مجازی از ابزارها و لوازم همراه دیجیتال و برنامک‌های کاربردی به جا می‌گذارد، مفهوم حریم خصوصی را با چالش اساسی روبرو نموده است. نگارنده به تفصیل بیان می‌دارد که الگوی زندگی سایبری امروزی امکان انزوا از این اسلوب حیاتی را از افراد سلب نموده اما در عین حال با اعلام مطالب فنی، ضمن توسعه بینش سایبری مخاطب نسبت به عمق و گستره میزان نظارت، روش‌هایی را برای ارتقاء نسبی امنیت و کاهش ردپاهای دیجیتالی پیشنهاد می‌دهد.

فصل سوم با عنوان «مهندسی اجتماعی» ضمن ارائه تعریفی از آن دال بر فریب افراد اعتماد کننده برای دور زدن کنترل های امنیتی فیزیکی و سایبری محافظت از داده، به تشریح مواردی از تکنیک‌های مهندسی اجتماعی و نیز حملات پیشرفته‌ای که مقدمات و مراحل اولیه آن‌ها از طریق مهندسی اجتماعی انجام می‌شود، اشاره می‌نماید.

در فصل چهارم با عنوان «ردیابی تلفن همراه» آسیب‌پذیری‌های ناشی از کاربری تلفن‌های همراه هوشمند تشریح و ضمن ورود به جزئیات برخی از مدل‌های رایج گوشی‌های تلفن همراه، به انواع مختلف آسیب‌های مربوط به ردیابی از طریق تلفن همراه، اعم از ردیابی خود گوشی، ردیابی توسط برنامک‌های داشبورد گوشی یا برنامک‌های کاربردی که کاربران با اختیار خود نصب و از آنها بهره‌برداری می‌کنند، عطف توجه گردیده است. در انتهای فصل ضمن تشریح یک پرونده قضایی در این رابطه، به قدیمی بودن قوانین ایالات متحده و ناکارآمد بودن آنها به منظور حفاظت از حریم خصوصی شهروندان اشاره گردیده است.

در فصل پنجم با عنوان «ردیابی فیزیکی دستگاه‌ها» ضمن اشاره به توسعه و فراگیری فن ابزارهای جدید قابل پوشیدن و نیز ابزارهای چی‌پی‌اس ردیابی دستگاه‌ها (نظیر خوردوها) یا سالمندان یا حیوانات خانگی، تهدیدات ناشی از این ابزارها مورد بررسی قرار گرفته‌اند. خدماتی که این قبیل ابزارها در اختیار افراد قرار می‌دهند، موجب استفاده روزافزون از آنها شده، غافل از اینکه این فن ابزارها حلقه محاصره افراد را تنگ‌تر کرده و تقریباً تردد و حضور آنها را بصورت نقطه‌ای در تمامی ساعات شبانه روز مقدور می‌سازند.

فصل ششم به «ردیابی ویدئو و وب کم» اختصاص یافته و امکان ثبت ویدئو و تصویر افراد را بر اساس وجود دوربین‌های متعدد امنیتی در اماکن عمومی و خیابان‌ها، همراه داشتن گوشی‌ها و لپ‌تاپ‌های مجهز به دوربین و خدمات امنیتی نظارت بر اماکن شخصی و منازل به بحث می‌گذارد. نگارنده نتیجه می‌گیرد تقریباً لحظه‌ای و مکانی وجود ندارد که تصویر شما در حال ثبت نباشد یا امکان چنین کاری دور از دسترس باشد. وی ادامه می‌دهد که همه این مسائل غیر از امکان ردیابی با دوربین‌های ماهواره‌ای قدرتمند توسط دولت یا آژانس‌های نظامی و اطلاعاتی است.

«سرقت داده و سوء استفاده از آن» عنوان فصل هفتم است که در آن ضمن تقسیم‌بندی داده به دو گونه ثابت و سیار، تهدیدات مربوط به هر کدام مورد بحث قرار می‌گیرد.

داده‌های ثابت از طریق سرقت فیزیکی تا نفوذ به دستگاه‌های نگهداری آنها و داده‌های سیار با تکنیک‌های مختلف سایبری در مسیر انتقال می‌توانند ربوده شوند. هر چند روش‌های فنی جرم‌شناسی قانونی می‌توانند تا حدود زیادی رد مهاجمان و سارقان اطلاعاتی را مشخص نمایند، اما این اقدامات تضمینی برای امنیت داده ایجاد نمی‌کنند.

در فصل هشتم برخی «روش‌های محافظت» مورد بررسی قرار گرفته و بر اساس ماهیت تهدیداتی که در فصول دوم تا هفتم به تفصیل مورد بحث واقع شد، ضمن معرفی روش‌هایی برای کاهش مخاطرات مجدداً تاکید گردیده که امکان تضمین امنیت کامل داده، دست‌نیافتنی است.

فصل نهم در واقع مقدمه بخش دوم کتاب بوده و اشاره کلی به فصل‌بندی ادامه کتاب و رئوس مطالب مورد بحث در فصل‌های بعدی خواهد داشت.

در فصل دهم با عنوان «پیوند زدن ممانعت و فریب کلاسیک با قلمروی امنیت سایبری» تلاش می‌شود ضمن اشاره به چهارچوب ممانعت و فریب در دنیای واقعی و در زمینه‌های کلاسیکی چون جنگ، دیپلماسی و ... ، این ادبیات و راهبردهای نسبتاً قدیمی آن، در بافتاری سایبری بومی‌سازی شده و به این حوزه بسط داده شوند. بر این اساس ماتریس ممانعت و فریب معرفی و تاکتیک‌ها، فنون و رویه‌های ممانعت و فریب سایبری در ساختار ماتریس یاد شده تشریح شده است. همچنین به الزامات سازمانی برنامه‌ریزی و اجرای عملیات موفقیت‌آمیز ممانعت و فریب سایبری نیز اشاراتی شده است.

«نفوذ، فریب و کارزارها» عنوان فصل یازدهم کتاب است که ضمن توجه به راهبردهای نفوذ سایبری که در سال‌های اخیر بسط و توسعه یافته‌اند، سطوح چهارگانه گام‌های تهاجمی، حمله‌ها، زنجیره‌های کشتار و کارزار را معرفی و به ارائه تحلیل‌هایی در خصوص طراحی و اجرای استراتژی‌های ممانعت و فریب سایبری، متناسب با هر کدام از این سطوح می‌پردازد. بر این اساس گزینه‌های ممانعت و فریب سایبری در هر مرحله در قالب مدلی جامع متشکل از فرآیندهای برنامه‌ریزی، آماده‌گری و اجرای عملیات فریب و ممانعت تشریح و طبق مدل

مزبور مراحل هر حمله سایبری و رفتار عاملان این حملات تشریح شده‌اند.

در فصل دوازدهم «مورد کاوی‌های ممانعت و فریب سایبری» مدنظر بوده و دو مطالعه موردی در حوزه فریب و ممانعت و حملات سایبری برای ارائه درک عملیاتی به خواننده از مفاهیم و روندهای فریب در حملات سایبری واکاوی شده است. مورد اول ماجرای حمله «استاکس نت» به تأسیسات غنی‌سازی اورانیوم جمهوری اسلامی ایران و گزارشات امنیتی مرتبط با این حمله ویژه سایبری است و مورد دوم، پرونده‌ای فرضی در خصوص جاسوسی سایبری است. پرونده نخست نحوه بکارگیری گسترده ممانعت و فریب تهاجمی در سطوح فنی، تاکتیکی، عملیاتی و راهبردی است و پرونده دوم استفاده از عناصر فریب و ممانعت سایبری در فرآیند تدافعی و مقابله با جاسوسی سایبری را نشان می‌دهد.

در فصل سیزدهم با عنوان «تمرین ممانعت و فریب سایبری» جزئیات یک آزمایش تحقیقی تحت عنوان اس‌ال‌ایکس با کمک آن تی‌های آبی، سرخ و سفید هر کدام نقش‌های مشخصی را عهده‌دار بوده و یک ماموریت یعنی جنگ سایبری را برگزار نموده‌اند، توضیح داده شده است. رویکرد اصلی این تمرین واکاوی میزان تاثیرگذاری افزودن فنون، تاکتیک‌ها و رویه‌های ممانعت و فریب به دفاع سایبری سنتی در مقابل نفوذ بوده و نشان می‌دهد که استفاده از فریب و ممانعت اولاً به چه نحوی در فرآیند دفاع سایبری مقدور بوده و ثانیاً تا چه اندازه می‌تواند این فرآیند را کارآمدتر سازد.

فصل چهاردهم با عنوان «ملاحظات، انطباق و اشتراک‌گذاری» در تبیین این موضوع است که عملیات فریب و ممانعت به هر علتی ممکن است با شکست کامل یا نسبی در تحقق اهداف از پیش تعیین‌شده مواجه گردد. در چنین موقعیت‌هایی چه باید کرد؟ انطباق‌پذیری و چالاکی در برنامه ریزی، آماده‌گری و اجرای عملیات فریب حیاتی هستند و طراحان فریب باید برای عکس‌العمل نسبت به شرایط نامطلوب نیز آمادگی داشته باشند. این مهم با شناسایی مخاطرات، پیامدهای ناخواسته، افشا و ناکامی عملیات فریب و داشتن طرحی برای این موقعیت‌ها مقدور خواهد بود. بر این اساس در این فصل برای مراحل

مختلف طراحی و اجرای عملیات فریب فنون، مزایا، چالش‌ها و معایب احتمالی متناظر معرفی و نهایتاً نیز مقوله استانداردسازی مفاهیم و رویه‌ها و به اشتراک‌گذاری تجارب بین سازمان‌ها و طرف‌های قابل اعتماد برای حصول درک و آگاهی موقعیتی جامع‌تر پیشنهاد گردیده است.

«مقابله با ممانعت و فریب» عنوان فصل پانزدهم کتاب است که در آن مفهوم ضد فریب و کاربرد آن در دفاع سایبری مورد بررسی قرار می گیرد. غیر از مقوله ممانعت و فریب در سا و کار دفاع سایبری، مفهوم ضد فریب نیز بر اساس مدلی که در این فصل ارائه گر یده منظور پرده برداشتن از عملیات فریب حریف مهاجم برای اهداف دفاع سایبری ارزشمند خواهد بو مهاجمین برای افزایش ضریب موفقیت طرح نفوذ و فرار از تور شناسایی مدافعین و اقدامات مقابله‌ای آنان، حملات خود را بر اساس فنون و تاکتیک‌های فریب و مقابله طراحی و عملیاتی می کنند. لذا شناسایی این اقدامات در مراحل پیش و پس از بهره‌برداری، مدافعین را در اتخاذ تدابیر و راهبردهای دفاعی موثرتر یاری خواهد نمود. یک مطالعه موردی در ارتباط با کاربست این مفاهیم علیه عملیات گسترده جاسوسی صنعتی و علمی چینی ها نیز برای تعمیق درک عملیاتی خوانندگان در انتهای فصل ارائه شده است.

فصل شانزدهم با عنوان «مدل بلوغ توانمندی» بحث تفصیلی در خصوص بلوغ توانمندی‌های فریب و ممانعت و در هر دو رویکرد تهاجمی و دفاعی سایبری را ارائه می‌دهد. در حقیقت تلاش می شود تا معیارها و سنجه‌هایی کاملاً ساختارمند و استاندارد شده از توانمندی عملیات فریب و ممانعت ارائه گردد تا خواننده قادر به ترسیم چارچوبی برای ارزیابی از آمادگی سازمان خودی یا تخمین توانمندی‌های رقبای فرضی باشد. همچنین کاربست این مدل که پنج سطح از بلوغ سازمانی در حوزه فریب و ممانعت را تبیین می‌کند، می‌تواند در نقش دستورالعملی برای تحکیم و ارتقاء توانمندی‌های راهبردی ممانعت و فریب سایبری مورد استفاده مدیران تحول در حوزه سایبری قرار گیرد.

در فصل هفدهم با عنوان «مدیریت چرخه حیات ممانعت و فریب سایبری» خود مقوله مدیریت عملیات فریب و ممانعت به لحاظ تفکیک اجزای چرخه حیات آن و تشریح هر کدام از گام‌های این چرخه مورد توجه قرار گرفته است. سطح بلوغ، سنجه‌ها، مشهودات و شاخص‌ها، زمینه‌سازی‌ها، فرآیندهای عملیاتی و مدل مدیریتی ابعاد شش‌گانه مدیریت چرخه حیات عملیات فریب و ممانعت هستند که در این بخش معرفی شده‌اند.

فصل پایانی نیز «نگاهی به آینده» موضوع و مسیرهای پیش روی عملیات ممانعت و فریب و روش‌های مرتبط با این حوزه داشته و گرایش بیشتر به مدل‌های نظریه بازی و مدل‌های زیستی و سیستم ایمنی فیزیولوژیک را بسترهای توسعه فراروی این حوزه معرفی می‌نماید.

امید است مطالعه این کتاب بتواند نگاه درست و عمیقی از تهدیدات سایبری و روش‌های کاهش و مدیریت تأثیرات مخرب آن را در سطوح مختلف فردی و مدیریتی و راهبردی در اختیار مخاطبان و جامعه علمی و حرفه‌ای مرتبط با این حوزه قرار دهد.

معاونت پژوهش و تولید علم

فهرست مطالب