جنگ سایبری

تکنیک‌ها، تاکتیک‌ها و ابزارها برای مهاجمان حوزه امنیت

مؤسسه آموزشی و تحقیقاتی صنایع دفاعی
حوزه نوآوری آرایه‌های دفاعی
دارای مجوز سازمانی نشر از شورای سیاست‌گذاری و نظارت بر انتشارات
مؤسسه آموزشی و تحقیقاتی صنایع دفاعی

سرشناسه : اندرس، جیسن Andress, Jason
عنوان و نام پدیدآور : جنگ سایبری: تکنیک‌ها و تاکتیک‌ها و ابزارها برای فعالان حوزه امنیت/ [تالیف جیسن اندرس، استیو وینترفلد]؛ مترجم طرح فراسازمانی فاوا و همکاران.
مشخصات نشر : تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی، حوزه نوآوری سازمان و مدیریت دفاعی، ۱۳۹۶.
مشخصات ظاهری : ۶۶۹ ص.
شابک : ۹۷۸۶۰۰۸۷۹۳۲۵۰
عنوان اصلی : Cyber warfare : techniques, tactics and tools for security practitioners, 2nd. ed, [2014].
عنوان دیگر : تکنیک‌ها، تاکتیک‌ها و ابزار امنیتی و کاربردی برای جنگ‌های سایبری.
عنوان دیگر : جنگ سایبری: (تکنیک‌ها، تاکتیک‌ها و ابزار برای دست‌اندرکاران امنیتی).
موضوع : جنگ اطلاعاتی — دستنامه‌ها — شبکه‌های کامپیوتری — تدابیر ایمنی — دستنامه‌ها
شناسه افزوده : وینترفلد، استیو Winterfeld, Steve
شناسه افزوده : موسسه آموزشی و تحقیقاتی صنایع دفاعی. طرح فراسازمانی فاوای نیروهای مسلح
شناسه افزوده : موسسه آموزشی و تحقیقاتی صنایع دفاعی. حوزه نوآوری آرایه‌های دفاعی
رده بندی کنگره : ۱۳۹۶ ۸ت۷۸ الف/U۱۶۳
رده بندی دیویی : ۳۵۵/۳۴۳ شماره کتابشناسی ملی: ۵۰۸۷۰۴۱

عنوان: جنگ سایبری، تکنیک‌ها، تاکتیک‌ها و ابزارها برای فعالان حوزه امنیت
مترجم: طرح فراسازمانی فاوا و همکاران
ویراستار و نظارت بر ترجمه و چاپ: طرح فراسازمانی فاوا
ناشر: مؤسسه آموزشی و تحقیقاتی صنایع دفاعی ـ حوزه نوآوری آرایه‌های دفاعی
آماده‌سازی چاپ: مدیریت دانش حوزه نوآوری آرایه‌های دفاعی
نوبت چاپ: اول ـ زمستان ۱۳۹۶
شمارگان: ۵۰۰ جلد
قیمت: ۴۰۰۰۰ تومان

نشانی: بالاتر از میدان نوبنیاد، پاسداران شمالی، نبش کوهستان هشتم، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی،
تلفن: ۲۲۸۰۸۷۰۷ نمابر: ۲۲۸۰۸۷۷۴

پیش گفتار

چرا یک کتاب درباره جنگ سایبری [illegible]؟

«امروزه مشخص شده است که تهدید سایبری به یکی از بزرگ‌ترین چالش‌های امنیتی ملی و اقتصادی تبدیل شده است که ما [illegible] آن مواجه هستیم.» ما به عنوان یک کشور یا یک دولت به اندازه کافی برای مقابله با این خطر آماده نیستیم [۱].

بر طبق گفته مدیر سازمان اطلاعات ملی آمریکا آقای «James Clapper»، تهدید جنگ سایبری که آمریکا با آن مواجه است در حال افزایش یافتن است و دشوار است که بتوان درباره تأثیر آن اغراق کرد. بسیاری از مؤسسات آموزشی هم در سطح نظامی و هم در سطح غیرنظامی با این سؤال مواجه هستند که «ما باید درباره امنیت سایبری به دانشجویان خود چه چیزی را آموزش دهیم؟» وقتی این دانشجویان در آینده در جایگاه خود به عنوان مدیر و یا افسر اطلاعاتی، نقش دفاع از کشور را بر عهده دارند باید از تهدیدات پایدار آگاه باشند.

امروزه به‌طور پیوسته مقیاس خطرات در حال تغییر کردن است و ما باید اقدامات متقابل و مأموریت‌های مختلف خود را از شناسایی سارقین گرفته تا شناسایی جرائم و جاسوسی‌ها در سطح ملی و شناسایی کرم‌های کامپیوتری مانند استاکس‌نت که هدف خرابکاری دارند، ادامه دهیم. حدود یک دهه قبل بود که تعدادی کودک تنها به علت هیجان ناشی از هک کردن، به سیستم‌ها حمله می‌کردند. سپس این عمل به‌عنوان یک عمل مجرمانه شناخته شد. در حال حاضر به نظر می‌رسد این قضیه بیشتر با انگیزه‌های اجتماعی، ایدئولوژی افراد و تهدیدات خودی مرتبط است. این کتاب توضیحات بسیار خوبی را درباره گستردگی خطرات موجود و چالش‌هایی که ما امروزه با آن‌ها مواجه هستیم فراهم می‌کند.

در ماه مه [سال ۲۰۱۱]، مجله‌ای به نام «the Atlantic Wire» گزارش کرد که چین در حال پیروز شدن در جنگ سایبری است؛ زیرا آن‌ها به برنامه‌های جنگی فیزیکی آمریکا دست پیدا کرده‌اند. همچنین ادوارد اسنودن ادعا کرده است که ایالات‌متحده و رژیم صهیونیستی با همکاری یکدیگر ویروس استاکس‌نت را علیه برنامه اتمی ایران نوشته‌اند. ما هنوز در حال تلاش برای فهمیدن چگونگی عملکرد این ویروس هستیم. درحالی‌که ویکی‌لیکس و گروه ناشناس (گروه عقیده محوری که سازمان‌هایی را که از ویکی‌لیکس حمایت نمی‌کنند، مجازات می‌کند) اخیرا اعلام کرده‌اند که سرقت برنامه احراز هویت دو عاملی[1] به‌شدت باعث ایجاد دلسردی شده است. اگر کنترل دسترسی از بین رود همه چیز از بین خواهد رفت. امروزه سرقت هویت به یک امر عادی تبدیل شده است که دیگر ارزش خبری ندارد. چند نفر از مردم در ایالات‌متحده اطلاعات هویتی آن‌ها به سرقت رفته است؟ بیشتر متخصصین می‌گویند که اطلاعات همگی مردم به سرقت رفته است. اطلاعات بسیار زیادی به سرقت رفته است که مجرمان حتی هنوز نمی‌دانند چگونه می‌توانند از آن‌ها استفاده

1 Two-factor authentication

کنند، ولی روزی بالاخره خواهند توانست از تمامی آن اطلاعات استفاده کنند. گروه‌های تبهکار، دانشمندان کامپیوتری را استخدام می‌کنند تا کلاه‌برداری‌های سایبری آن‌ها را انجام دهند. اصطلاح جنگ سایبری در حال تبدیل شدن به بحث همیشگی در گفتگوهای امنیت ملی است. امنیت سایبری مسئله‌ای است که در سطح شخصی، مانند کاربران اینترنتی، می‌تواند بر روی زندگی ما تأثیر بگذارد و در سطح دفاع ملی به‌عنوان یک تهدید پیشرفته و پایدار برای کشور مطرح است.

چرا باید این کتاب را بخوانید؟

همگی ما باید خبر داشته باشیم که اطلاعات ما با آن‌ها مواجه هستند را درک کنیم تا بتوانیم تصمیمی آگاهانه بگیریم و گام‌های لازم برای امن کردن اطلاعات خود را برداریم.

اینترنتی که در خانه از آن استفاده می‌کنید تا با دوستانتان از طریق اسکایپ[1] صحبت کنید و یا بازی برخط انجام دهید و نامه‌های الکترونیکی خود را ارسال کنید، ممکن است برای انجام اعمال مجرمانه، انجام جاسوسی بین‌المللی و یا حتی در مبارزه با نوع جدیدی از جنگ سایبری مورد استفاده قرار گیرد.

این نوع جدید از اینترنت امروزی برای هر یک از ما حیاتی است در سطح شخصی و چه در سطح ملی مهم است. جنگ سایبری بیشتر در سطح ملی است. برای اینکه وزارت دفاع (آمریکا) چه عملی را انجام می‌دهد تمرکز می‌کند.

ما حتی یک هفته را هم بدون شنیدن اخبار درباره جنگ سایبری و اینکه گروه‌های هکری در حال گسترش نرم‌افزاری‌های مخرب در اینترنت هستند، پشت سر نخواهیم گذاشت. جنگ سایبری به‌وسیله نشان دادن ارتباط تمامی حملات با

1 Skype

یکدیگر و نحوه عمل کردن این تهدیدات، خطر موجود را برای مردم قابل درک می‌سازد.

اگر شما برای دولت ایالات‌متحده کار می‌کنید یا اینکه می‌خواهید بدانید که دولت آمریکا چه کاری را انجام می‌دهد تا به تهدیدات سایبری پاسخ دهند، در فصل اول (جنگ سایبری چیست) با جزئیات کامل به این موضوع پرداخته می‌شود. این کتاب به شما نشان خواهد داد که چگونه حملات سایبری و دفاع در مقابل آن تمامی حوزه‌های جنگی کلاسیک مانند زمینی، دریایی، هوایی، فضایی (مشترک با نیروی هوایی) و سایبری که توسط فرماندهی سایبری آمریکا (USCYBERCOM) سازمان‌دهی می‌شود) را درگیر می‌کند.

جنگ سایبری دکترین نظامی که در حال توسعه می‌باشد را پوشش می‌دهد و تاکتیک‌ها، تکنیک‌ها و روال عملیات شبکه‌های کامپیوتری (CNO[1]) که شامل حمله، دفاع و بهره‌برداری[2] (این یک اصطلاح نظامی برای عملیات جاسوسی و یا شناسایی است) و همچنین جنبه جدیدی از مهندسی اجتماعی است را سازمان‌دهی می‌کند. از نقطه نظر شخصی، آسان است که درباره مهندسی اجتماعی بخوانیم و با خود بگوییم که «بله درست است ولی من در شبکه‌های اجتماعی مابین سایر مردم هستم.» چندی پیش یک شخصیت ساختگی به نام «Robin Sage» توسط یک محقق امنیتی ساخته شد تا بفهمد که چه مقدار اطلاعات را می‌توان از طریق فیس‌بوک جمع‌آوری کند. در ادامه در فصل‌های این کتاب درباره اینکه جنگ سایبری چیست و اینکه چگونه جنگ سایبری انجام می‌شود توضیح خواهیم داد. همان‌طور که نویسنده در این کتاب مسائل قانونی و اخلاقی پیرامون این میدان نبرد جدید را مطرح می‌کند، دلیل اینکه چرا جنگ سایبری روی می‌دهد مشخص

1 Computer Network Operations
2 Exploit

می‌شود. سپس، این کتاب چالش‌های پیش‌روی فضای سایبر را آنالیز و تعریف می‌کند. درنهایت به تمایلات موجود پیرامون این موضوع می‌پردازد.

جنگ سایبری به خوانندگان یک درک بنیادی قوی از تهدیدات موجود که هر هفته در اخبار مشاهده می‌کنند، می‌دهد. در اینجا به این نکته می‌پردازیم که چرا جنگ سایبری مهم است. در ابتدای این پیشگفتار من با خود گفتم که «چرا من سرگیجه دارم؟» «چون مسائل بسیار زیادی پیرامون این موضوع وجود دارد که من نمی‌توانم همگی آن‌ها را پیگیری کنم؟» جواب این سؤال خیر است. چیزی که باعث گیج شدن من شد این است که ما داریم درباره موضوعی گفتگو می‌کنیم که ۱۳ سال قبل وقتی من مسئول رشد جنگ سایبری در سازمان دفاع ضد موشکی بودم مطرح شد. امروزه کلمات اختصاری پیرامون این موضوع بیشتر شده‌اند و همچنین پول بیشتری در این زمینه هزینه می‌شود. ولی هیچ‌یک از مسائل پایه‌ای و بنیادی تغییر نکرده است. در آن زمان، روسیه و احتمال این بود که توافقات بین‌المللی لازم بر سر این موضوع که با جنگ سایبری باید به‌عنوان یک سلاح راهبردی رفتار کرد را کسب کند. ولی ما گوش نکردیم. من گمان می‌کنم دلیل مخالفت ما این بود که فکر می‌کردیم که فناوری و تکنیک‌های ما پیشرفته‌تر و برتر هستند. علاوه بر این، بسیاری از مردم با خود می‌گفتند «آیا واقعا جنگ سایبری یک مسئله مهم است؟» بسیار دیگری از مردم حتی از این موضوع اطلاعی نداشتند. از دید آن (به شوخی) اگر این موضوع به گاو بازان و تیم «Redskin» ربطی ندارد چرا باید مهم باشد؟ ولی ما چیزی را فراموش کرده‌ایم. ما چیزهای زیادی داریم که می‌توانیم از دستشان دهیم. کشور آمریکا بیشترین اطلاعات برخط[1] را نسبت به هر کشور دیگری در اینترنت دارد و این امر باعث می‌شود که ما به بزرگ‌ترین هدف برای حملات سایبری تبدیل شویم. ما این فرصت را در پیش از یک دهه قبل داشتیم که برای همکاری

1 On-line

دولت، صنعت و بخش خصوصی گفتگوها را شروع کنیم. ما این فرصت را داشتیم که تا توافقات بین‌المللی بر سر این موضوع را ایجاد کنیم. ولی ما این فرصت‌ها را از دست دادیم. شواهد قانع‌کننده‌ای وجود دارد که نشان می‌دهد تهدید سایبری وجود دارد. ما باید خودمان را تعلیم دهیم و قانون‌گذاران خود را تشویق کنیم که قوانینی را برای این موضوع ایجاد کنند. ما باید دولت خود را قانع کنیم که دلارهای مالیاتی ما را به‌جای انجام سرمایه‌گذاری‌های بیهوده، در زمینه سایبری خرج کند. کتاب جنگ سایبری به شما اجازه می‌دهد که دانش خود را در این زمینه افزایش دهید و تصمیم بگیرید که در این زمینه کشور باید چه عملی را انجام دهد و از خطری که در صورت انجام ندادن عملی برای مقابله با جنگ سایبری با آن مواجه خواهید شد مطلع شوید. بیش از یک دهه است ما فرصت خود را برای انجام اقدام جامع در سطح بین‌المللی از دست دادیم و ما مجبور هزینه‌های زیادی شدیم. این بار ما می‌خواهیم چه کاری انجام دهیم؟

این متن توسط «Stephen Northcutt» نوشته شده است.

منابع

[1] President Barack Obama. Remarks by the president on securing our nation's cyber infrastructure [home page on the Internet]. Washington, DC: The White House, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-OurNations-Cyber Infrastructure/; 2010 [accessed 15.02.10].

[2] Allen V. Cyber warfare threats to U.S. are increasing: top spy [home page on the Internet]. New York: Thomson Reuters, http://www.reuters.com/article/2011/02/10/us-usa-intelligence-cyberspaceidUSTRE7194E320110210; 2010 [accessed 15.02.10].

فهرست مطالب