عباس معلم

آشنایی با فناوری امنیت سایبری

راهنمای انتخاب ابزارهای مناسب

دکتر مؤید محسنی

انتشارات ترجمک

آشنایی با فناوری های امنیت سایبری

راهنمای انتخاب ابزارهای امنیت سایبری صحیح

عباس معلم

آشنایی با فناوری‌های امنیت سایبری:

راهنمای انتخاب ابزارهای امنیت سایبری مناسب

ترجمه

دکتر مؤید محسنی

ویراست اول

زمستان ۱۴۰۳

انتشارات ترجمک

شماره کتابشناسی ملی	:	۹۸۷۸۵۵۹
شابک	:	۳۵۰۰۰۰۰ریال: 978-622-7855-89-0
عنوان و نام پدیدآور	:	آشنایی با فناوری‌های امنیت سایبری: راهنمای انتخاب ابزارهای امنیت سایبری مناسب/ عباس معلم؛ ترجمه موید محسنی.
مشخصات نشر	:	همدان، ترجمک، ۱۴۰۳
مشخصات ظاهری	:	ک، [۱۹۶] ص.: مصور.
شناسه افزوده	:	عنوان اصلی: Understanding cybersecurity technologies : a guide to selecting the right cybersecurity tools, 2022.
شناسه افزوده		شبکه‌های کامپیوتری -- تدابیر ایمنی (-- Computer networks Security measures)، امنیت کامپیوتر (Computer Security)
شناسه افزوده	:	محسنی، موید، ۱۳۵۶–، مترجم
رده بندی کنگره	:	TK5105/59
رده بندی دیویی	:	۰۰۵/۸

شناسنامه کتاب

نام کتاب: آشنایی با فناوری های امنیت سایبری: راهنمای انتخاب ابزارهای مناسب

ترجمه: دکتر موید محسنی

ناشر: انتشارات ترجمک

صفحه آرایی: انتشارات ترجمک

طراحی جلد: محمدحسین گیوی

نوبت چاپ: اول، ۱۴۰۳

قیمت (چاپی): ۳۵۰۰۰۰ تومان

قیمت (ایبوک): ۱۲۵۰۰۰ تومان

چاپ: گروه نشر الکترونیک ترجمک

شابک (پرینت): ۰-۸۹-۷۸۵۵-۶۲۲-۹۷۸

شابک (ایبوک): ۶-۹۰-۷۸۵۵-۶۲۲-۹۷۸

تلفن تماس: ۰۹۱۸۱۵۰۶۱۰۰

تارنمای اینترنتی: https://tarjomac.com

ISBN : 978-622-7855-89-0

ISBN : 978-622-7855-90-6

نویسنده:

دکتر عباس معلم

Abbas Moallem

مترجم:

دکتر موید محسنی

Moaied Mohseni

شابک اورجینال:

ISBN: 978-0-367-45745-7 (hbk)

ISBN: 978-1-032-15784-9 (pbk)

ISBN: 978-1-003-03842-9 (ebk)

شابک ترجمه فارسی:

شابک (پرینت): ۹۷۸-۶۲۲-۷۸۵۵-۸۹-۰

شابک (ایبوک): ۹۷۸-۶۲۲-۷۸۵۵-۹۰-۶

سال انتشار: ۲۰۲۳ – سی آر سی. پرس (چاپ اول)

انتشارات ترجمک: سال ۱۴۰۳

همدان، صندوق پستی ۱۱۷-۶۵۹۱۵ tarjomac@gmail.com

مقدمه

حملات سایبری به شرکت ها، موسسات دولتی و افراد به طور تصاعدی در حال افزایش است. در عین حال، تعداد شرکت‌های کوچک و بزرگی که انواع راه‌حل‌ها را پیشنهاد می‌دهند نیز رو به افزایش است. از آنجایی که شرکت‌ها برای محافظت از خود در مقابل حملات سایبری به راه‌حل‌های تکنولوژیک تکیه می‌کنند، شناخت و انتخاب راه‌حلی مناسب از میان همه راه‌حل‌های ارائه‌شده، متخصصان، مدیران شرکت‌ها و تازه واردان حوزه امنیت سایبری را با چالش مهمی مواجه می سازد.

در کنفرانس RSA 2019، یک نمایشگاه امنیت اطلاعات که در سانفرانسیسکو، کالیفرنیا برگزار شد، بیش از ۷۰۰ شرکت محصولات خود را در زمینه امنیت سایبری به نمایش گذاشتند. آیا این بدان معناست که آنها بیش از ۷۰۰ فناوری منحصر به فرد را ارائه می دهند؟ بدیهی است که نه. تعداد فناوری های واقعی مرتبط با امنیت سایبری بسیار کمتر از تعداد شرکت‌هایی است که آنها را ارائه می دهند. بسیاری از این شرکت‌ها از فناوری‌های یکسانی استفاده می‌کنند و آن‌ها را به‌صورت بسته‌بندی متفاوتی برای فروش عرضه می کنند، که گاهی اوقات حتی تفاوت‌های خیلی جزئی با هم دارند. مثلا شرکت های زیادی وجود دارند که راه حل های آنتی‌ویروس ارائه می دهند. آیا آنها از فناوری های مشابه یا متفاوتی استفاده می کنند؟ اگر متفاوت است، پس آن تفاوت ها در چیست؟ اگر کسی بخواهد یک راه حل آنتی ویروس را انتخاب کند، مهمترین معیار این است که بفهمد چه راه حل های تکنولوژیکی در محصول استفاده می شود. در طول تحقیقی درباره راه‌حل‌های فناوری امنیت سایبری، من کتاب‌ها، مجلات، وبلاگ‌ها، مقالات و وب‌سایت‌های شرکت مربوط به فناوری امنیت سایبری را برای توضیحات محصول بررسی کردم. پس از صرف زمان قابل توجه برای پیمایش، مرور و خواندن این منابع، آموختم که:

- اکثر کتاب هایی که توسط کارشناسان مختلف نوشته شده اند، فوق العاده فنی هستند و برای همه سطوح حرفه امنیت سایبری چندان قابل درک نیستند.
- کتاب های موجود اغلب به دلیل تغییرات سریع حوزه امنیت سایبری قدیمی هستند.
- کتاب ها اغلب بیش از حد کلی هستند و شامل توصیف آسان برای درک فناوری‌ها نیستند.

- مجلات فنی، مقالات یا وبلاگ ها عمدتاً توسط تأثیرگذاران نوشته می شوند، به این معنی که اطلاعات ارائه شده همیشه عینی یا قابل اعتماد نیستند. این منابع اغلب شرکت ها، راه حل ها را رتبه بندی می کنند و بر ارائه توضیحات کلی از راه حل ها تمرکز می کنند.
- شرکت ها تنها توضیحات راه حل را با مواد بازاریابی عمومی و بدون توضیح عمیق و قابل درک از فناوری ها ارائه می دهند. گاهی اوقات توضیحات عمومی هستند و به سادگی ویژگی های محصول را فهرست می کنند – نه فناوری مورد استفاده برای ارائه آن ویژگی‌ها.

پس از مطالعه مطالب شرکت‌های مختلف حاضر در کنفرانس، تصمیم گرفتم از هر یک از فروشندگان در نمایشگاه محصولات امنیت سایبری توضیح شفاهی بخواهم. در حالی که به نمایش های بازاریابی آنها در سالن های نمایشگاه گوش می دادم، متوجه شدم که اکثر افرادی که در این سخنرانی ها شرکت می کردند برای به دست آوردن اطلاعات با مشکل مواجه بودند. این یک تجربه بسیار ناامید کننده بود.

ارائه ها بسیار عمومی بودند، حتی بیشتر از خواندن مطالب. گاهی اوقات نیز محتوا توسط افرادی ارائه می شد که خودشان متخصص فناوری نبودند. اسلاید پاورپوینت های عمومی اغلب با چند سؤال مسابقه همراه بود که به شما امکان می‌داد جایزه نمادین دریافت کنید.

پس از آن تجربه، من در جلسات مدیریت شرکت‌های مختلف درباره راه‌حل‌های امنیت سایبری تحقیق کردم و به این نتیجه رسیدم که در بسیاری از موارد، تنها مدیران امنیتی شرکت‌های مربوطه کاملا آگاه و مسلط بوده و درک قوی از موضوع دارند. در بقیه مواقع، آشکار بود که متصدیان به خوبی آگاه نبودند و دانش عمیقی از فناوری‌های واقعی نداشتند.

به دنبال این تجربه، تصمیم گرفتم خودم را به چالش بکشم و یک راهنمای قابل درک از فناوری‌های امنیت سایبری ایجاد کنم که بر فناوری‌های موجود و در راه‌حل‌های مختلف استفاده می‌شود، بدون تمرکز بر شرکت‌هایی که چنین فناوری‌هایی را ارائه می‌کنند.

اولین قدم ارائه دسته بندی و توصیف قابل اعتماد و قابل درک برای هر گروه از فناوری‌ها است.

نیت این کتاب کمک به همه متخصصان تازه کار در زمینه امنیت سایبری، دانشجویان و متخصصان است، تا از محتوا برای آموزش مخاطبان خود در مورد مبانی راه حل های ارائه شده استفاده کنند.

پس از طبقه بندی مختصر فناوری های اصلی (فصل ۱)، هر فصل صرفاً بر روی یک نوع یا گروهی از فناوری ها تمرکز خواهد کرد. هدف ایجاد فصول مختصر و قابل هضم، اجتناب از اصطلاحات فنی تا حد امکان و تمرکز بر فناوری های منبع باز است. محتوای هر فصل منسجم است: پس از مقدمه و پیشینه تاریخی، نحوه عملکرد فناوری‌ها را شرح می‌دهم، فناوری‌های اصلی را در هر گروه توضیح می‌دهم، مزایا

و معایب اصلی آن فناوری‌ها را بیان می‌کنم، محصولاتی را که از آن فناوری‌ها استفاده می‌کنند (در صورت لزوم) فهرست می‌کنم. و با یک نتیجه گیری کوتاه فصول ختم می شوند. برای کمک به درک فناوری‌ها، از تمثیل ها و یک تصویر بصری (نقشه درختی با شاخه‌های مختلف) برای کمک به خوانندگان غیر فنی و ارائه یک تصویر ذهنی استفاده می‌کنم. علاوه بر این، به منظور شفاف سازی اصطلاحات، کلیه اصطلاحات و تعاریف فنی استفاده شده در هر فصل به همراه نام افراد ذکر شده در کتاب در بخش واژه نامه گنجانده شده است.

عباس معلم

نویسنده

دکتر عباس معلم (Abbas Moallem)، دکتری حرفه ای، مشاور و استاد کمکی در دانشگاه ایالتی سن خوزه، کالیفرنیا است که در آنجا تعامل انسان و کامپیوتر، امنیت سایبری، تجسم اطلاعات و عوامل انسانی را تدریس می کند. او رئیس برنامه HCI-CPT، کنفرانس بین المللی HCI برای امنیت سایبری، حریم خصوصی و اعتماد است.

دکتر معلم ویراستار کتاب تعامل انسان با کامپیوتر و امنیت سایبری و نویسنده کتاب آگاهی از امنیت سایبری در میان دانشجویان و اساتید دانشگاه است. او همچنین ویراستار یک سری کتاب از CRC Press با عنوان عنصر انسانی در سیستم‌های اسمارت و هوشمند است.

فهرست مندرجات در یک نگاه

عنوان صفحه

فهرست مندرجات کتاب

عنوان صفحه

فصل ۱

دسته‌بندی فناوری‌های امنیت سایبری

۱–۱ مقدمه

امنیت سایبری[1] یک حوزه علمی رو به رشد است که از انواع بسیار متنوعی از فناوری‌ها تشکیل شده است که برای محافظت از سیستم ها در برابر انواع مختلف حملات، برخی آشنا و برخی ناشناخته، استفاده می شود. به دلیل پیچیدگی جنبه های در حال تحول این حوزه، هیچ دسته‌بندی استانداردی از فناوری های حفاظتی وجود ندارد. دسته‌بندی فناوری های سایبری به درک بهتر نحوه عملکرد این فناوری ها کمک می کند. در این فصل، پس از مرور برخی از دسته‌بندی‌های مختلف موجود، روشی را ارائه می‌دهم که فناوری‌های سایبری محافظ بازنگری شده در این کتاب را طبقه‌بندی کرده‌ام.

۱–۲ دسته‌های مختلف فناوری سایبری

فناوری های مورد استفاده در امنیت سایبری به طرق مختلفی دسته‌بندی شده است. از دیدگاه تحقیقاتی، موضوعات امنیت سایبری به شرح زیر طبقه بندی می شوند [۱]:

۱. امنیت سایبری کاربردی
۲. علم داده های امنیت سایبری
۳. آموزش و تعلیم امنیت سایبری
٤. وقایع امنیت سایبری
٥. مدیریت و سیاست امنیت سایبری
٦. فناوری امنیت سایبری
۷. امنیت سایبری انسانی و اجتماعی
۸. نظریه ها در امنیت سایبری

[1] Cybersecurity

از نقطه نظر عملی، یک نوع طبقه بندی معمولاً بر اساس نوع تهدیدات و اثرات مورد نظر آنها است. در این دسته، تهدیدها به دو گروه طبقه بندی می شوند [۲]:

۱. تکنیک های حمله
۲. اثرات تهدید

نوع دیگری از طبقه بندی بر اساس نوع محافظت سایبری است. سپس فناوری های حفاظتی را می توان به چهار گروه طبقه بندی کرد:

۱. سیستم معماری
۲. نوع شناسایی (تشخیص)
۳. اکوسیستم
٤. نوع داده

فناوری‌های امنیت سایبری را می‌توان بر اساس مؤلفه‌هایی که هر فناوری قرار است از آنها محافظت کند نیز طبقه‌بندی کرد. این طبقه بندی شامل گروه های اصلی زیر است:

۱. شبکه (Network)
۲. اپلیکیشن (Application)
۳. نقطه پایان (Endpoint)
٤. داده (Data)
٥. هویت (Identity)
٦. دیتابیس (Database)
۷. فراساختار (Infrastructure)
۸. موبایل (Mobile)
۹. ابر (کلود) (Cloud)
۱۰. پشتیبان (Backup)

نوع دیگری از دسته بندی بر اساس انواع راه حل های امنیتی است. طبقه بندی مبتنی بر راه حل یک شیوه تجربی‌تر برای دسته‌بندی فناوری‌های سایبری است. در این دسته‌بندی راه‌حل‌ها به گروه‌های زیر دسته‌بندی می شوند:

۱. مدیریت هویت و دسترسی
۲. مدیریت ریسک و رعایت

۳. رمزگذاری
٤. پیشگیری از بین رفتن داده (DLP)
٥. مدیریت واحد تهدید (UTM)
٦. دیوار آتش (فایروال)
۷. راه حل های آنتی ویروس / ضد بدافزار
۸. سیستم تشخیص تهاجم (IDS)/سیستم جلوگیری از تهاجم (IPS)
۹. بازیابی سوانح
۱۰. کاهش حملات انکار توزیع شده خدمات (DDoS).
۱۱. فیلتر کردن وب

۱–۳ دسته‌بندی فناوری

برای این کتاب، من از طبقه بندی بر اساس راه حل های تکنولوژیک موجود استفاده می‌کنم. آنها به ۱۶ دسته اصلی گروه‌بندی می شوند. در هر فصل، من نمای درختی فناوری‌های هر گروه پیشرو را ارائه می‌دهم. دسته‌بندی در این کتاب شامل گروه‌های زیر است (شکل ۱–۱):

۱. رمزگذاری
۲. احراز هویت
۳. بیومتریک
٤. فایروال
٥. حفاظت نقطه پایان
٦. شناسایی فیشینگ
۷. شناسایی ویروس (معمولاً با دسته حفاظت نقطه پایان در یک گروه واحد گذاشته می شود)
۸. محافظت در مقابل بدافزار
۹. اینترنت اشیا
۱۰. امنیت شبکه
۱۱. ردیابی مکان
۱۲. نظارت یا مراقبه
۱۳. تهدید داخلی
۱٤. تشخیص تهاجم
۱٥. اسکن آسیب پذیری
۱٦. تست نفوذ

شکل ۱-۱ دسته‌بندی فناوری امنیت سایبری بر اساس راه حل های تکنولوژیک موجود