تیم قرمز حرفه‌ای

انجام تعاملات امنیت سایبری موفقیت‌آمیز

فصل هشتم: تیم بنفش

مهدی لقایی
سهیل هاشمی

۸

فصل هشتم: تیم بنفش

عملیات تیم بنفش به هر روش، فرایند یا فعالیتی گفته می‌شود که با بهره گیری از تعامل بین جنبه‌های آبی و قرمز امنیت سازمانی انجام می‌شود. منظور از "قرمز" همه تلاش‌های امنیت تهاجمی یا شبیه سازی حمله است. "آبی" به هر تلاشی گفته می‌شود که شامل اقدامات دفاعی صورت گرفته توسط سازمان است. به باور من، وقتی قابلیت‌های دفاعی و تهاجمی در ترکیب با هم در قالب یک عملیات تیم بنفش استفاده می‌شوند، می‌توانند حد نهایی ارتقای امنیت سازمانی را به تصویر بکشند. رسیدن به این هدف بدون چالش نیست و فعالیت‌های تیم بنفش هم انواع مختلفی دارند - برخی از این فعالیت‌ها قرمزتر و برخی به آبی نزدیک‌تر هستند. در این فصل به بررسی چالش‌های تیم بنفش پرداخته و نمونه‌هایی از فعالیت‌های تیم بنفش را مرور می‌کنیم که به نظر من کارآمد و مؤثر هستند.

چالش‌ها

خیلی از مشکلات تیم قرمز در عملیات تیم بنفش هم مشاهده می‌شود و بیشتر این مشکلات به پرسنل ارتباط دارند. اجرای موفقیت آمیز و حرفه‌ای عملیات تیم قرمز به تنهایی کار دشواری است. اضافه شدن یک محیط عملیاتی مشارکتی که در آن کارشناسان تهاجمی و دفاعی باید با یکدیگر همکاری کنند هم این چالش را سخت‌تر می‌کند. چالش‌های تیم قرمز می‌توانند باعث دشواری یا کاهش اثربخشی این ارزیابی‌ها شوند اما مشکلات مربوط به پرسنل می‌توانند باعث خروج کامل تعاملات تیم بنفش از مسیر اصلی شده و حتی روابط کاری را به حدی تیره کنند که گزینه تیم بنفش کاملاً حذف شود.

مشکلات مربوط به افراد

هنگام اجرای عملیات تیم قرمز برای یک مشتری چندین بار با شرایط خاصی روبرو شدم که به روابط بین کارمندان ارتباط داشت. پس از ماه‌ها درخواست از سمت مدیریت سازمان مشتری برای اجرای تعاملاتی شبیه به تیم بنفش، تیم قرمز با تیم‌های آبی و نظارتی سازمان تماس گرفت. هدف این بود که اعضای تیم آبی سازمان را بیشتر با فعالیت‌های خودمان آشنا کنیم تا به آنها برای یافتن و نظارت بر فعالیت‌های خودمان کمک کنیم. متأسفانه آنها از این اطلاعات برای پیدا کردن و نظارت بر ما و همچنین ایجاد مانع برای فعالیت‌های تیم قرمز ما استفاده کردند تا در جلسه با مدیریت سازمان به گیر انداختن ما ببالند و دائماً مانع از انجام فعالیت‌های ما می‌شدند. این خبر به گوش یکی از مدیران فنی که مسئول تیم قرمز بود رسید؛ او از اینکه ما گیر افتاده و بی‌کفایت تلقی شده بودیم، ناراحت شد و این موضوع باعث بحث شدید او با همتای

خودش در تیم آبی شد. اینکه یک یا دو نفر از افراد نتوانستند حین عملیات تیم قرمز رفتار حرفه‌ای را رعایت کنند کل این تعامل و چندین هفته رابطه کاری را تحت تأثیر قرار داد و در نهایت با فعالیتی که تقریباً هیچ مزیتی به غیر از خودستایی چند نفر نداشت، باعث اتلاف منابع و زمان بسیار زیادی شد.

در یک سازمان دیگر، یک عملیات تیم بنفش مفیدتر - اما باز هم خسته کننده - را اجرا کردیم که به دلایل مختلف، تقریباً به نتیجه‌ای مثل مثال قبلی رسید. تیم قرمز تصمیم به بررسی برخی هشدارها و قوانین نظارتی مورد استفاده تیم آبی برای ایمن سازی سازمان گرفته بود و واکنش به حادثه را به شیوه‌ای نیمه خودکار شروع کرد. تیم آبی کاملاً با این ایده موافقت کرد و پس از اعلام رضایت، تیم قرمز ارزیابی نیمه خودکار قابلیت‌های نظارتی را آغاز کرد. متأسفانه ادامه ماجرا بدتر از آنچه پیش بینی شده بود پیش رفت در حالی که از قبل برنامه ریزی شده بود که مدیریت ارشد سازمان در جریان این مأموریت قرار گرفته و زمان ارایه نتایج به آنها هم مشخص شده بود. گرچه بر سر بخش آبی از این تلاش تیمی موافقت شده بود و هیجان زیادی درباره آن وجود داشت اما شکست غیرمنتظره کارمندان نظارتی و ارایه‌ای که پس از آن برای مدیریت سازمان انجام دادند، برای این تیم به شدت خجالت آور بود. فعالیت تیم بنفش از نظر درک ضرورت تقویت وضعیت امنیتی سازمان توسط مدیریت سازمان نتیجه خوبی داشت. اما از آنجایی که عملکرد تیم آبی ضعیف‌تر از پیش بینی بود، از نظر شخصی و حرفه‌ای خجالت زده شدند و اینکه حالا وضعیت امنیتی سازمان از قبل بهتر شده بود، از نظر آنها اهمیت چندانی نداشت. این یک نمونه از شرایط سخت‌تری است که ممکن است حین اجرای عملیات تیم بنفش ایجاد شود چون این بار هیچ یک از افراد دخیل عملکرد غیر حرفه‌ای نداشتند و هیچ چیز بر خلاف برنامه توافق شده انجام نشد اما باز هم نتیجه این فعالیت برای عده‌ای نامطلوب بود.

همانطور که این مثال‌ها نشان می‌دهند، مشکل افراد در عملیات تیم بنفش بسیار وسیع و تأثیرگذار است. درست همانطور که روابط خصمانه با مشتری و کارهای غیرحرفه‌ای از سمت مشتری و کارمندان مشتری می‌تواند بر عملیات تیم قرمز تأثیرات نامطلوبی داشته باشد، این مسائل می‌توانند برای تیم بنفش هم مخرب باشند. اگر افراد تیم‌های قرمز یا آبی دستور کار خودشان را برای تعاملات تیم بنفش داشته باشند، این مسئله می‌تواند همه تلاش‌ها را بی‌اثر کند. بدتر اینکه، حتی وقتی همه افراد دخیل در این فرایند کارشان را درست انجام دهند، تصورات غلط یا نتایج غیرمنتظره می‌توانند مزایای تیم بنفش و ادامه فعالیت‌های آن را تحت تأثیر قرار دهند. حتی زمانی که بر سر اجرای عملیات توافق شده باشد، در صورتی که نتایج ارزیابی به نفع

یک گروه رقم بخورد ممکن است بین افراد اختلاف ایجاد شود. مشکلات مربوط به افراد فراتر از مسائل مربوط به کارمندان امنیتی دخیل در این فرایند هستند. ممکن است مدیریت به نحوی از نتایج تیم بنفش استفاده کند که روابط خصمانه بین افراد تشدید شود.

مثلاً در مثال‌های قبلی اگر مدیر تیم آبی درخواست مساعدت از مدیران سطح بالای سازمان داشته باشد اما نتیجه گیری این باشد که تیم قرمز خوب است یا حتی بهتر و حرفه‌ای‌تر است و به این دلیل تیم قرمز پشتیبانی مالی بیشتری کسب کند، ممکن است شرایط به شدت سخت شده و برخوردهای نامناسبی ایجاد شود.

نیازهای مشتری

مثل چالش‌های فنی و رویه‌ای که برای اجرای موفقیت آمیز عملیات تیم قرمز وجود دارد، ممکن است تیم بنفش هم برای برآورده ساختن نیازهای مشتریان با چالش روبرو شود. موضوع این کتاب، عملیات تیم قرمز حرفه‌ای است و معمولاً در این زمینه سمت آبی باز هم مشتری است. در تیم بنفش، مشتری سازمان است و ارایه دهندگان خدمات، هر دو تیم آبی و قرمز هستند. تجربه نشان داده که معمولاً مشتری چنین دیدگاهی نسبت به این فرهنگ ندارد و تیم بنفش را یکی از جنبه‌های خدمات تیم قرمز در نظر می‌گیرد که تیم آبی را درگیر کرده و به بهبود و ارتقای عملکرد آن کمک می‌کند. به ویژه در صورت استفاده از خدمات اجرا کنندگان تست نفوذ برون سازمانی، شرایط معمولاً به همین صورت است. در کنار انبوه موانع و مشکلات برای اجرای موفقیت آمیز یک ارزیابی امنیت تهاجمی به صورت برون سازمانی، باید یکی از بخش‌های سازمان که احتمالاً روابط خصمانه‌ای با شما دارد را دعوت به همکاری کنید. بدتر اینکه، در این شرایط تیم قرمز نمی‌تواند از بخش آبی سازمان کمک بگیرد. بنابراین تیم قرمز در شرایطی قرار می‌گیرد که موفقیت آن در ارایه خدمات تیم بنفش برای مشتری وابسته به استفاده از داشته‌های تیم آبی است که احتمال موفقیت در به کار گرفتن و همکاری آنها سخت بوده و برخلاف نیروهای تیم قرمز، با مشتری رابطه تجاری ندارند و انگیزه موفقیت آنها کمتر است.

چنین دلایلی باعث شده که احتمال موفقیت تیم بنفش در سازمان‌ها بزرگ یا سازمان‌هایی که وضعیت امنیتی کامل‌تری دارند، بیشتر باشد. احتمالاً چنین سازمان‌هایی تجهیزات لازم برای هر دو نوع تیم‌های قرمز و آبی را دارند. تیم بنفش با اجرای ارزیابی‌هایی که در بلندمدت و به صورت دوره‌ای انجام می‌شود بهترین نتیجه را فراهم می‌کند و برای سازمان‌های بزرگتر امکان ایجاد چنین شرایطی بیشتر است. این به آن معنا نیست که سازمان‌های کوچک با منابع کمتر امکان تحقق مزایای مشارکتی تیم بنفش را ندارند بلکه باید این تلاش را به گونه‌ای برنامه ریزی

کرد که به نتایج نامطلوب منجر نشود. نیازهای مشتری نحوه شکل گرفتن عملیات تیم بنفش را تعیین می‌کنند و ارایه دهنده باید اطمینان حاصل کند که عملیات تیم قرمز متناسب با وضعیت امنیتی سازمان انجام می‌شود. وقتی سازمان قابلیت‌های نظارتی کمی دارد، همکاری تیم قرمز و آبی متفاوت با شرایطی است که در آن قابلیت‌های نظارتی سازمان کامل‌تر بوده و نیاز به ارزیابی مشارکتی بخشی از دستگاه امنیتی دارد. بخش شکل دهی به محدوده عملیات تیم بنفش نسبت به عملیات تیم قرمز معمولی حساس‌تر است و باید در برقراری ارتباط با سازمان مشتری احتیاط زیادی داشت تا عملیات تیم بنفش به موفقیت رسیده و در بلند مدت مورد پذیرش و استقبال قرار بگیرد.

انواع تیم بنفش

تیم‌های قرمز و آبی می‌توانند به روش‌های زیادی برای بهبود امنیت سازمان با یکدیگر همکاری کنند. همانطور که پیش از این اشاره شد، فعالیت‌های تیم بنفش شامل تلاش‌های منسجم نیروهای تیم آبی و قرمز است. به طور کلی می‌توان تعاملات رایج تیم‌های بنفش را به دو دسته تقسیم کرد یعنی: دسته‌ای که در آنها یکی از طرفین از فعالیت‌های یک طرف خاص که می‌تواند مهاجم یا میزبان باشد، آگاهی ندارد و دسته دوم تعاملاتی که در آنها هر دو طرف تا حدودی از فعالیت‌های یکدیگر آگاهی دارند. پس از اجرای عملیات تیم بنفش هم یک ارزیابی از آنچه در این عملیات صورت گرفته انجام می‌شود و در این مرحله دو طرف با یکدیگر برای از بین بردن نقطه ضعف‌های شناسایی شده همکاری می‌کنند. در ادامه به بررسی برخی روش‌های اجرای عملیات تیم بنفش می‌پردازیم که من شخصاً تجربه انجام آنها را دارم و به نظر من تأثیر زیادی در تقویت امنیت سازمانی دارند.

آگاهی متقابل

می‌توان گفت که کلاسیک‌ترین نمونه از تعاملات تیم بنفش مواردی هستند که در آنها هر دو تیم آبی و قرمز نسبت به فعالیت‌های طرف مقابل و نقش آن در تعامل، حداقل مقداری اطلاعات دارند اما معمولاً این درک به یک میزان است. مزیت استفاده از این نوع عملیات تیم بنفش این است که معمولاً احتمال خصمانه شدن آن کمتر است چون هیچ یک از تیم‌ها اطلاعات زیادی را از تیم مقابل مخفی نمی‌کند. اعضای تیم قرمز در جریان هستند که اعضای تیم آبی از حضور و فعالیت آنها آگاهی دارند و اینکه این آگاهی چقدر است؛ اعضای تیم آبی هم از فعالیت‌ها و اهداف برنامه ریزی شده تیم قرمز اطلاع دارند. یکی از معایب این روش این است که معمولاً در

آن واقع گرایانه‌ترین شبیه سازی حمله توسط تیم قرمز اجرا نمی‌شود. در بیشتر مواقع، این شرط برای اجرای چنین عملیاتی مورد پذیرش قرار می‌گیرد.

به عنوان یکی از اعضای تیم قرمز در چنین تعاملاتی، ممکن است نسبت به تیم آبی چند مسئولیت داشته باشید. ارزیان تیم قرمز باید به غیر از تهیه یادداشت‌های عملیاتی مناسب، پیش از شروع بهره برداری به اعضای تیم آبی اطلاع رسانی کنند. در واقع اعضای تیم قرمز باید همان جزئیاتی که در یادداشت‌های عملیاتی ثبت می‌شود را در اختیار اعضای تیم آبی قرار دهند و در صورت امکان این کار را به صورت بلادرنگ انجام دهند. این یعنی باید به اعضای تیم آبی درباره مبدأ، مقصد، زمان تقریبی و سپس زمان دقیق بهره برداری و همچنین نوع اکسپلویت اجرا شده اطلاع داد. این تاکتیک به تیم آبی امکان می‌دهد که قابلیت‌های نظارتی و دفاعی خودشان را به صورت بلادرنگ تحلیل و اصلاح کنند. اگر ابزارهای نظارتی به موقع درباره اجرای اکسپلویت هشدار صادر نکنند و یا فایروال یا ضد ویروس با موفقیت آن را شناسایی نکنند، تیم آبی بلافاصله متوجه این موضوع می‌شود و می‌تواند همزمان با ادامه عملیات تیم بنفش، راهکارهای مناسب را برای رفع مشکل اجرا کند. به همین ترتیب، اعضای تیم آبی هم باید به تیم قرمز درباره شناسایی فعالیت‌های این تیم در شبکه و وضعیت سیستم‌های تشخیص نفوذ میزبان محور اطلاع رسانی کنند تا اعضای تیم قرمز هم بتوانند روش‌ها و شگردهای خودشان را اصلاح و تقویت کنند. وقتی در عملیات تیم بنفش هر دو تیم آبی و قرمز از فعالیت‌های طرف مقابل آگاهی دارند، هر دو تیم می‌توانند همزمان با اجرای ارزیابی، اصلاحات لازم را در روش‌های خودشان ایجاد کنند.

بی‌اطلاعیِ میزبان

در یکی دیگر از انواع رایج ارزیابی‌های تیم بنفش، سیستم‌های دفاعی میزبان محور تیم آبی اطلاعات زیادی از فعالیت‌های تیم قرمز ندارند. در چنین مواقعی، فقط یکسری نشانه مبهم در رابطه با فعالیت‌های تیم قرمز در اختیار تیم آبی قرار گرفته و سعی بر این است که با تلاش تیم آبی برای جستجو، شناسایی یا پیشگیری از فعالیت‌های تیم قرمز، توانمندی‌های این تیم تقویت شود. احتمالاً اطلاعات ارایه شده برای تیم آبی در حد تاریخ شروع و پایان فعالیت تیم قرمز است و ممکن است اطلاعات اختصاصی‌تری مثل بخشی از سازمان که تحت بررسی تیم قرمز قرار دارد یا هدف آنها از اجرای حمله هم مشخص شود. تیم قرمز از اینکه دقیقاً چه اطلاعاتی در اختیار تیم آبی قرار می‌گیرد، آگاه است و با تمام تلاش سعی می‌کند از شناسایی شدن پیشگیری کند. اجرای عملیات تیم بنفش به این روش به تیم قرمز امکان می‌دهد که شبیه سازی واقع گرایانه‌تری از حمله ایجاد کرده و پیچیدگی حمله را افزایش دهد. ایراد این روش این است که احتمال ایجاد

محیط خصمانه بین تیم قرمز و آبی با این روش بیشتر می‌شود چون این دو تیم را در تقابل با یکدیگر قرار می‌دهد.

بی‌اطلاعیِ مهاجم

یکی از سناریوهایی که احتمال اجرای آن کمتر است، بی‌اطلاعیِ مهاجم است. در چنین شرایطی، تیم قرمز تقریباً هیچ اطلاعاتی از قابلیت‌ها یا فعالیت‌های تیم آبی ندارد. همچنین تیم قرمز در جریان نیست که تیم آبی در رابطه با اقداماتش اطلاعات دریافت می‌کند. چنین شرایطی باعث می‌شود که تیم قرمز به صورت بلادرنگ تحت نظارت باشد و دستگاه دفاعی سازمان اطلاعات زیادی از فعالیت این تیم داشته باشد. در این روش، تیم قرمز بدون ایجاد مانع به کار خود ادامه می‌دهد و در انتها تیم آبی گزارشی در رابطه با چگونگی پیشرفت و فعالیت‌های تیم قرمز ارایه می‌دهد به همراه اطلاعات به دست آمده در اثر نظارت بر شبیه سازی حمله از ابتدا تا پایان آن.

تیم آبی می‌تواند چالش‌هایی در مسیر تیم قرمز قرار دهد تا واکنش این تیم را بررسی کند. این چالش‌ها می‌توانند شامل قرار دادن پست‌های شنود مورد استفاده ابزارهای دسترسی از راه دور در لیست سیاه، ایمن سازی حساب‌های مورد استفاده تیم قرمز برای حرکت در شبکه یا پاکسازی برخی سیستم‌ها از ابزارهای مورد استفاده تیم قرمز باشد. از آنجایی که تیم قرمز در جریان نیست که به صورت لحظه‌ای تحت نظارت قرار دارد، طوری به این اقدامات واکنش نشان می‌دهد که انگار جزء یک ارزیابی معمولی هستند. اطلاعات به دست آمده توسط تیم آبی در این روش، برای آشنایی با طرز فکر مهاجمان و واکنش طبیعی هکرهای اخلاقی بسیار مفید هستند. اگر چنین فعالیتی به عنوان بخشی از یک عملیات درون سازمانی بزرگتر انجام شود، به تیم قرمز هم امکان می‌دهد که با دسترسی به گزارش نهایی تیم آبی، از چشم‌انداز و دیدگاه مدافع اطلاع پیدا کند. طبیعتاً اجرای چنین عملیات تیم بنفشی در مواقعی که بین اجرا کننده تست نفوذ و سازمان، رابطه ارایه دهنده و مشتری وجود دارد ممکن نیست اما یکی از روش‌های خیلی خوب برای تقویت مهارت‌های تیم‌های قرمز و آبی درون سازمانی است.

تست دست قرمز (مُچ‌گیری)

تست مچ‌گیری یا به اصطلاح دست قرمز بر اساس اصطلاح "دست قرمز" (کنایه از آغشته به خودن بودن) طراحی شده که مفهوم آن گیر انداختن است. حین اجرای تست مچ گیری، هدف ارزیابی گیر انداختن تیم قرمز توسط تیم آبی است. این نوع عملیات تیم بنفش به دلایل مختلف بر همه مراحل ارزیابی متمرکز می‌شود و در هر مرحله با واکنش‌های متفاوتی همراه است. تست از قبل گیر انداختن تیم قرمز و شناسایی اقدامات این تیم شروع می‌شود. من هم در چنین

ارزیابی‌هایی حضور داشته‌ام و به نظرم این ارزیابی‌ها برای سازمان مشتری بسیار مفید هستند. همانطور که قبلاً اشاره شد، چنین تست‌هایی می‌توانند منجر به ایجاد درگیری بین تیم‌ها شوند.

مسلماً می‌توان تست مچ گیری را به صورت دستی و همچنین با اتوماسیون اجرا کرد. حین اجرای چنین ارزیابی‌هایی، اعضای تیم ارزیابی به تدریج امنیت عملیاتی و شگردهای خودشان را کاهش می‌دهند تا وقتی که تیم قرمز اقدامات آنها را شناسایی کنند. در این مرحله، عملیات تیم بنفش می‌تواند وارد یکی از این دو مسیر شود: تیم آبی که تیم قرمز را شناسایی کرده، فعالیت‌های تیم بنفش را متوقف کرده و با تیم قرمز در رابطه با آنچه تا آن مرحله رخ داده و علت شناسایی تیم قرمز گفتگو کند. یا تیم آبی به تیم قرمز درباره شناسایی شدن این تیم اطلاع می‌دهد و تیم قرمز به تدریج اقدامات مخفی و شگردهای خودش را تقویت می‌کند تا زمانی که تشخیص فعالیت‌های این تیم از فعالیت‌های مجاز ممکن نباشد. این دو مرحله معمولاً تکرار می‌شود و طی آن تیم آبی سعی می‌کند عملکرد خود را در زمینه اطلاع و شناسایی فعالیت‌های تیم قرمز بهبود ببخشد. یکی از مشکلات این روش این است که راهکار قابل تکرار یا قابل دفاعی برای ارتقای عملکرد تیم آبی نیست و ممکن است برای هر سازمانی کارایی نداشته باشد.

یکی دیگر از روش‌های اجرای تست مچ گیری، اتوماسیون آن با کمک مهارت‌های هکرهای اخلاقی است. در چنین ارزیابی‌هایی عامل انسانی تقریباً به صورت کامل حذف می‌شود و هدف، بیشتر ارزیابی قابلیت‌های پیشگیرانه و نظارتی موجود سازمان است.

اولین بار که شاهد پیاده سازی این تکنیک بودم، این کار توسط تیم قرمز یک سازمان بسیار بزرگ انجام شده بود. پس از اینکه تقریباً قابلیت دسترسی به همه دستگاه‌های مرکز داده سازمان را ارزیابی کردیم، آماده اجرای تست مچ گیری خودکار شدیم. مهارت اصلی، انتخاب نقطه اجرای ابزار است. برخی اهداف از داخل خود مرکز داده انتخاب شدند، برخی مخصوص برقراری ارتباط با مرکز داده بودند و برخی در مناطق غیرنظامی و سایر زیرمجموعه‌های مدیریتی محدوده هدف قرار داشتند. ابزاری که ما نصب کردیم، یک مجموعه فعالیت امنیت تهاجمی داشت که سطوح پیچیدگی متنوعی داشتند. از جمله اضافه کردن یک کلید برای یک کاربر **SSH**، ماندگار کردن یک باینری یا اسکریپت، ایجاد یک کاربر و اقدامات مشابه دیگر. این فعالیت‌ها به ترتیب و بر اساس احتمال شناسایی (از کمترین به بیشترین احتمال) - و همزمان روی همه دستگاه‌ها - اجرا شدند. پس از تکمیل اجرای این ابزارها، با تیم آبی صحبت کردیم تا ببینیم چه فعالیت‌هایی در نرم‌افزار نظارتی آنها شناسایی شده، از اجرای کدام فعالیت‌ها پیشگیری شده و چه هشدارهایی ایجاد شده بودند. به این ترتیب، تیم آبی درک واضح‌تری نسبت به توانمندی‌های دفاعی خودشان پیدا کردند.

در برخی موارد، اقداماتی که تیم آبی تصور می‌کرد صددرصد متوجه آنها می‌شود، نادیده گرفته شده بودند و دلیل این موضوع پیکربندی اشتباه تپ‌های شبکه و مشکلات دیگر بود.

می‌توان این تست‌های مچ گیری را همراه با عملیات تیم آبی انجام داد که در آن این تیم قوانین دفاعی و نظارتی خود را از قبل مشخص کرده و تیم قرمز هم کارهایی را انجام می‌دهد که برای شناسایی شدن توسط دستگاه‌های دفاعی طراحی شده‌اند. این استراتژی یک تصویر فوری از نیازهای سازمان در زمینه مقابله با آسیب‌پذیری‌ها فراهم می‌کند چون هشدارهایی که نادیده گرفته می‌شوند ارتباط مستقیمی با فعالیتی دارند که تیم آبی تصور می‌کند با آن مقابله کرده است. گزینه بعدی این است که تیم قرمز در گزارش نهایی، اقدامات انجام شده را ثبت کرده و آنها را با تیم آبی مرور کند تا توانایی‌های این تیم برای شناسایی چنین اقداماتی تقویت شود. با این کار می‌توان ترتیب اقدامات اصلاحی را بر اساس میزان خطر فعالیت‌های انجام شده مشخص کرد چون باید فعالیت‌های بسیار خطرناکی که شناسایی نشده‌اند، به عنوان اولویت مورد بررسی و تحلیل قرار بگیرند.

دو روش قبلی بررسی شده بیشتر به اقدامات امنیتی امضا محور می‌پرداختند که در آنها تیم آبی درون سازمانی نقطه ضعف‌های خودش را در زمینه ثبت یا مقابله با برخی اقدامات شناخته شده شناسایی می‌کند. یکی از مفاهیم جدیدی که اخیراً با یکی از همکاران به آن پرداختیم، استفاده از فناوری یادگیری ماشینی برای ارزیابی خودکار دستگاه امنیتی یک سازمان بود. بدون شک این موضوع با مبحث اصلی این کتاب که مربوط به هک اخلاقی است فاصله دارد اما اشاره به آن در کنار این مفاهیم مربوط به مچ گیری در تیم بنفش می‌تواند مفید باشد. در این روش، یک ابزار در نقاط مختلف سازمان و اینترنت نصب می‌شود که ترافیک مبنای شبکه سازمان را شنود کرده و بر اساس آن آموزش می‌بینند. سپس این ابزار بر عکس نرم‌افزارهای نظارتی اکتشافی (یا هیوریستیک) عمل می‌کند و شروع به ارسال ترافیک خودش می‌کند. همچنان که شباهت ترافیک ارسال شده توسط این ابزارها به خط مبنای ترافیک شبکه کمتر و کمتر می‌شود، نرم‌افزارهای نظارتی با سطوح پیچیدگی مختلف باید کم کم این ترافیک ناهنجار را در نقاط مختلف شناسایی کنند. با قرار دادن و اجرای چنین ابزاری در نقاط حساس ترافیک شبکه، سازمان می‌تواند مشخص کند که آیا ابزارهای نظارت بر ترافیک اکتشافی یا حتی امضا محور طوری پیکربندی شده‌اند که ترافیک ناهنجار را شناسایی کنند یا خیر.

گرفتن و رها کردن

تست مچ گیری بیشتر متمرکز بر بهبود یا شناسایی خلأهای موجود در روش‌های مورد استفاده تیم آبی است. تست گرفتن و رها کردن یکی از انواع مأموریت‌های تیم بنفش است که با هدف ارزیابی توان ارتجاعی عملیات تیم قرمز و عملکرد تیم آبی در شناسایی و پیگیری فعالیت‌های تیم قرمز طراحی شده است. طی چنین مأموریت‌هایی، تیم قرمز در یک مرحله شناسایی می‌شود. وقتی این اتفاق رخ می‌دهد، به تیم قرمز در رابطه با اینکه چه اقدامی باعث شناسایی آنها شده، اطلاع رسانی می‌شود و سپس یک فرصت کوتاه در اختیار تیم قرمز قرار می‌گیرد؛ پس از آن تیم آبی شروع به قرنطینه ابزارهای مورد استفاده تیم قرمز و بیرون انداختن آنها از شبکه می‌کند. باید فاصله بین اطلاع رسانی و اجرای فعالیت‌های دفاعی یا شکار با فاصله بین فعال شدن هشدار در اثر تشخیص یک اقدام خاص در دستگاه‌های نظارتی، توجه یک تحلیلگر انسانی به آن و شروع فرایند واکنش به حادثه تناسب داشته باشد. این "گرفتن" می‌تواند ارسال یک شبیه سازی شده هشدار یا شناسایی واقعی فعالیت‌های تیم قرمز توسط تیم آبی باشد. رها کردن هم فرصتی است که به تیم قرمز برای پیشگیری از گیر افتادن دوباره به همان روش و تلاش برای پایدار کردن حضور این تیم در شبکه داده می‌شود.

مزیت این روش این است که تیم قرمز می‌تواند هر فعالیت ممکنی را برای ارتقای قدرت تاب آوری خودش انجام دهد تا حضور خود را در سازمان پایدار کند. بعلاوه، تیم آبی هم واکنش واقع گرایانه به حادثه را تمرین می‌کند که در آن فعالانه سعی دارد شبکه را از مهاجمی که در جریان هست شناسایی شده، پاکسازی کند. بین همه روش‌های بررسی شده برای اجرای عملیات تیم بنفش، این روش به تیم‌های قرمز و آبی امکان می‌دهد که خلاقانه‌تر عمل کرده و فرایندهای مورد استفاده خودشان را تقویت کنند. باز هم احتمال اجرای این روش در سازمان‌هایی که تیم قرمز و آبی درون سازمانی دارند بیشتر است. به نظر من، این روش برای اجرای عملیات تیم بنفش بسیار مفید است و در آن مفهوم شبیه سازی حمله و ارزیابی واکنش یک سازمان به طور کامل اجرایی می‌شود.

همچنین روش گرفتن و رها کردن یک نکته بسیار ارزشمند را در رابطه با فعالیت‌های تیم قرمز، تیم آبی، تیم بنفش و در مجموع امنیت تهاجمی آشکار می‌کند یعنی اینکه شناسایی و گیر انداختن به معنای خنثی سازی کامل تهدید نیست. بسیاری از مواقع در حالی که عملیات همچنان در حال اجرا است، تیم آبی به ما اطلاع می‌دهد که چون ما را شناسایی کرده، عملیات به پایان رسیده است. طبق تجربه شخصی من، ممکن است هشدار یک فعالیت ساعت‌ها - یا

حتی روزها - پس از تکمیل آن فعالیت ایجاد شود و تقریباً در همه موارد، شناسایی آن فعالیت به تنهایی مانع از ماندگار شدن حضور مهاجمان نمی‌شود. فرض کنید که یک تیم آبی متوجه فعالیت ما برای اجرای یک اکسپلویت ارتقای دسترسی خطرناک روی میزبانی شود که در آن در جستجوی اطلاعات هستیم اما این شناسایی دو ساعت پس از اجرای اکسپلویت و یک ساعت پس از تمام شدن کار ما با آن سیستم صورت گرفته باشد؛ در این صورت این اقدام تیم آبی این به معنای شکست دادن تیم ما نیست. احتمالاً در این بازه زمانی اطلاعات مورد نظر مهاجم به دست آمده یا مهاجم موفق به نفوذ به سایر دستگاه‌ها شده است. به نظر من، کارشناسان امنیت دفاعی و تهاجمی باید درک کنند که حین اجرای یک ارزیابی و یا در شرایط واقعی، در صورتی که فرایند واکنش به حادثه قادر به ریشه کنی مهاجم در سازمان نباشد، شناسایی فعالیت مهاجم بی‌فایده خواهد بود. این تصور تیم آبی که به دلیل تشخیص یک فعالیت، ارزیابی انجام شده پیشرفته و حرفه‌ای نبوده یا یافته‌های بعدی تیم قرمز بی‌فایده هستند، دیدگاه بسیار ناامید کننده‌ای است. من بارها با چنین شرایطی برخورد داشته‌ام که در آن هدف اصلی درک نشده است. چنین مأموریت‌هایی فرصت بسیار خوبی برای یک سازمان هستند تا با محدودیت‌های خود آشنا شده و واکنش به حادثه را در مقابل مهاجمی تمرین کند که برخلاف هکرهای واقعی، قصد انتشار داده‌ها یا افشای آسیب‌پذیری‌های سازمان را ندارد.

هکر مفید

راحت‌ترین و دوستانه‌ترین روش پیاده سازی فعالیت‌های تیم بنفش، روشی است که پس از یک ارزیابی امنیت تهاجمی و حین رسیدگی به یافته‌ها انجام می‌شود. در این روش گزارش نتایج یا بازخوردهایی که مهاجم پس از اجرای یک عملیات تیم بنفش هدفمند ارایه می‌دهد می‌توانند برای پیاده سازی استراتژی اصلاح و رفع آسیب‌پذیری بسیار مفید باشند. با وجود چنین بازخوردهایی می‌توان مطمئن شد که مدافعان طوری به نتایج رسیدگی می‌کنند که در نهایت به شکست دادن مهاجمان واقعی کمک می‌کند نه مهاجمان شبیه سازی شده. همچنین در این روش می‌توان به صورت مؤثر فهرست یافته‌ها و ترتیب رسیدگی به آنها را اولویت بندی کرد. حین اجرای این مأموریت‌های تیم بنفش، بارها مشاهده شده که کارمندان بخش امنیت سازمان مشتری ایده‌هایی برای پرداختن به یافته‌ها مطرح کرده‌اند که منجر به توقف حمله تیم قرمز شده اما مشکل اصلی را ریشه کن نمی‌کنند. این رویکرد شبیه به درمان علائم بیماری به جای رسیدگی به علت اصلی بیماری است. در ادامه چند مثال واقعی را بررسی می‌کنیم که در آنها راهکار اولیه

مطرح شده توسط کارمندان امنیت با هدف رسیدگی به علائم پیشنهاد شده نه ریشه کن کردن مشکل اصلی.

در مورد اول، از محصولات امنیتی سازمان هدف برای گسترش آلودگی در سطح سازمان استفاده شد. یکی از این محصولات، نرم‌افزار مدیریت پیکربندی سازمانی بر اساس لینوکس بود که بخش‌های عمده‌ای از سازمان را به طور مرکزی مدیریت می‌کرد. مثال بعدی نرم‌افزار ضد ویروس مخصوص سیستم‌عامل ویندوز بود که به صورت مرکزی توسط یک سرور مدیریت می‌شد. در رابطه با نرم‌افزار لینوکس، استفاده مجدد از اعتبارنامه‌های کاربری امکان دسترسی از راه دور را فراهم می‌کرد و قابلیت ارتقای سطح دسترسی به تیم قرمز امکان می‌داد که در سرور مدیریت پیکربندی سازمان مستقر و پایدار شود. پس از آن، اعضای تیم توانستند تغییراتی در سازمان ایجاد کنند مثل نصب درهای پشتی، تغییر رمز عبور و اقدامات دیگر که همگی باعث فراهم شدن دسترسی ممتاز به همه نودهای تحت مدیریت می‌شوند. در میزبان‌هایی با سیستم‌عامل ویندوز، تکثیر یک حساب کاربری نیمه ممتاز روی یک سیستم، به تیم ارزیابی امکان داد تا به سرور مدیریت ضدویروس نفوذ کنند. سپس این تیم توانست رمزهای کنسول مدیریت تحت وب ضد ویروس را که روی این سیستم ذخیره شده بودند استخراج کرده و پس از ورود به این کنسول باینرهای دلخواهی را با سطح دسترسی سیستمی روی همه سیستم‌های موجود در آن دامنه از جمله کنترل‌گر دامنه اجرا کند. در هر دو حالت، کارمندان بخش امنیتی سازمان مشتری راهکارهایی را پیشنهاد دادند که متمرکز بر رسیدگی به علائم نفوذ بودند. مثلاً برای مشکل مربوط به لینوکس، پیشنهاد آنها ارتقای نسخه هسته و تغییر اعتبارنامه‌های کاربری دخیل در این فرایند بود. برای مشکل ویندوز هم توصیه نصب جدیدترین نسخه از نرم‌افزار ضد ویروس مطرح شد که توانایی بیشتری در مبهم سازی رمزعبور کنسول تحت وب داشت. در هر دو مثال، ارزیابان تیم قرمز توصیه‌هایی را برای رسیدگی به نقطه ضعف‌های واقعی موجود در دستگاه امنیتی سازمان مطرح کردند. در هر دو مورد لازم بود که ابزار مدیریت بسیار قدرتمند مورد استفاده سازمان از سایر سیستم‌ها تفکیک شده و برای آن از روش احرازهویت متفاوتی استفاده شود. مسئله اصلی ضرورت تفکیک سیستم‌های قدرتمند مذکور بود؛ سایر آسیب‌پذیری‌ها فقط امکان دسترسی به این سیستم‌ها را برای تیم ارزیابی فراهم می‌کردند. این به آن معنا نیست که نباید توصیه‌های کارمندان بخش امنیت سازمان را پیاده سازی کرد چون این توصیه‌ها هم مهم بودند. اما شباهت طرز فکر تیم قرمز به مهاجمان واقعی منجر به مطرح شدن ایده‌های دیگری شد که نه یک مسیر نفوذ خاص، بلکه انواع حملات را خنثی می‌کنند.

مثال بعدی مربوط به یک مرکز داده تحت لینوکس است. تیم قرمز با به دست آوردن دسترسی ممتاز ریشه[1] به یک سیستم خاص و استفاده از همان حساب ریشه برای دسترسی به سایر سرورهای لینوکس، به کل مرکز داده نفوذ کرد. تیم امنیت سازمان فقط قابلیت دسترسی سطح ریشه به SSH را غیرفعال کرده و مسیر مورد استفاده تیم قرمز را نادیده گرفت. در جلسات بعدی با تیم آبی، تیم قرمز به آنها اطلاع دادند که فقط با استفاده از یک حساب کاربری دیگر توانسته‌اند از راه دور وارد سیستم شده و بعد به صورت محلی دوباره به حالت ریشه جابجا شوند تا هر ابزار دلخواهی را نصب کنند چون رمز حساب ریشه در همه سیستم‌ها ثابت مانده و تغییر نکرده بود. تیم قرمز توصیه کرد که قابلیت انتقال کاربرانی با SSH به سطح ریشه غیرفعال شود یا اعتبارنامه‌های کاربر ریشه در سرورهای مختلف متفاوت باشد تا از استفاده مجدد از آنها پیشگیری شود.

آخرین مثال ما در زمینه تفاوت بین توصیه‌های تیم قرمز و تیم آبی و مزیت استفاده از هر دو در قالب تیم بنفش، مربوط به اجرای باینری است. در یکی از ارایه‌ها، تیم قرمز اعلام کرد که توانسته با استفاده از کارهای زمانبندی شده در سیستم‌عامل ویندوز، یک ابزار با پسوند exe. را اجرا کند. مدافعان اعلام کردند که می‌توانند برای مواقعی که از کارهای زمانبندی شده برای اجرای یک باینری exe. جدید استفاده می‌شود، یک امضای مخصوص بنویسند. این راهکار هم ارزشمند بود اما فقط به یک آسیب‌پذیری خاص می‌پرداخت نه ریشه اصلی. تیم قرمز به کارمندان امنیت سازمان توضیح داد که می‌توانستند یک dll. بنویسند و آن را با زمانبندی rundll.exe اجرا کنند یا حتی از یک پسوند دیگر مثل tlb. استفاده کنند. مشکل اصلی این بود که کارهای زمانبندی شده اجازه اجرای باینری با دسترسی سطح سیستمی را داشتند و تیم قرمز با تیم آبی برای ریشه کن کردن تهدید اصلی همکاری کرد.

صرف نظر از مثال‌های ارایه شده، باید دقت داشت که طراحی استراتژی‌های ریشه کنی و رسیدگی به آسیب‌پذیری‌ها توسط کارمندان امنیت سازمان به همراه تیم ارزیابی که تفکر تهاجمی دارند، بسیار مفید است. هیچ محدودیتی برای روش‌های اجرای عملیات تیم بنفش وجود ندارد و برای پیاده سازی آن در هر سازمانی باید بهترین راه بهره برداری از این مفهوم شناسایی شود تا به بهبود وضعیت کلی امنیت سازمان، ارتقای مهارت‌های تیم‌های آبی و قرمز و درک بهتر طرز فکر طرف مقابل کمک کند.

---

[1] root

خلاصه فصل هشتم

در این فصل به بررسی مفهوم تیم بنفش، چالش‌های آن و برخی از روش‌های اجرای فعالیت‌های تیم بنفش پرداختیم. همچنین مزایا و معایب انواع مختلف روش‌های اجرای عملیات تیم بنفش هم مورد بررسی قرار گرفت تا بهترین شرایط استفاده از آنها مشخص شود.

در نهایت سعی شد با مرور یکسری مثال واقعی، اطلاعات ارایه شده در این فصل بهتر به ذهن مخاطبان منتقل شود.

• تیم قرمز حرفه‌ای • مهدی لقایی • سهیل هاشمی

این کتاب به عنوان یک منبع برای افرادی نوشته شده که قصد اجرای مانورهای حرفه‌ای تیم قرمز را دارند؛ همچنین افرادی که از خدمات آنها استفاده می‌کنند. قرار نیست متن این کتاب هک کامپیوتر یا سازمان‌ها را به شما آموزش دهد بلکه به شما آموزش می‌دهد که چطور این کار را به روشی بهتر و طوری که منجر به ارتقای امنیت سازمان شود انجام دهید. این کار مستلزم کسب مهارت‌هایی فراتر از مهارت‌های شیرین هک برای اجرای ارزیابی های امنیتی تهاجمی است. چه به دنبال استخدام هکرهای اخلاقی باشید و چه به دنبال همکاری با آنها و چه خودتان یک هکر اخلاقی باشید، پس از مطالعه این کتاب باید درک بهتری از مهارت‌های لازم برای استفاده از شبیه‌سازی تهدیدات سایبری جهت کاهش ریسک پیدا کنید.