تیم قرمز حرفه‌ای

- مهدی لقایی
- سهیل هاشمی

فصل هفتم: گزارش نویسی

فهرست مطالب

۷

فصل هفتم: گزارش نویسی

می‌توان گفت که "برقراری ارتباط"، عنوان مناسب‌تری برای این فصل است. در صورت ضعف در انتقال نتایج ارزیابی به مشتری طوری که امکان ارتقای وضعیت امنیت سازمان فراهم شود، داشتن مهارت‌های هک عالی و شگردهای استثنائی هم بی‌فایده خواهد بود. حتی در مواقعی که تیم قرمز قصد ارایه گزارش به مخاطبان فنی‌تر را داشته باشد، به احتمال بسیار زیاد این افراد فاقد طرز فکر امنیت تهاجمی هستند و یافته‌های تیم قرمز را از منظر متفاوتی نگاه می‌کنند. بعلاوه، در بیشتر مواقع، گزارش تیم قرمز به مدیریت سطح بالای سازمان تحویل داده می‌شود تا تصمیم گیری‌های اقتصادی لازم را در رابطه با اصلاح و رفع مشکلات شناسایی شده انجام دهند. این مخاطبان که اطلاعات فنی کمتری داشته و مسئول تصمیم گیری هستند، معمولاً یک خلاصه از فعالیت‌ها دریافت می‌کنند یا گزارش تیم قرمز را پس از بازبینی توسط کارمندان امنیت داخلی تحویل می‌گیرند. در هر صورت، اگر مخاطبان گزارش ارزیابی درباره مزایای اقتصادی رسیدگی به یافته‌های تیم قرمز توجیه نشوند، کل ارزیابی تلاشی بیهوده خواهد بود که نه به سازمان مشتری کمکی می‌کند و نه برای امنیت تهاجمی انگیزه تجاری ایجاد می‌کند. در این فصل به بررسی اطلاعات مهمی می‌پردازیم که باید در گزارش پایان ارزیابی به آنها اشاره شوند. همچنین توصیه‌هایی در رابطه با روش‌های مؤثر انتقال گزارش ارزیابی به مخاطبان در سازمان مشتری مطرح می‌کنیم.

موارد لازم

معمولاً گزارش دهی از طریق یک ارایه مختصر یا گزارش مکتوب انجام می‌شود. در ادامه فصل به مشخصات یک خلاصه خوب اشاره خواهد شد؛ بخش‌های فعلی این فصل مربوط به خود سند گزارش هستند. کاملاً قابل درک است که چرا باید در گزارش انتهای ارزیابی به یافته‌ها اشاره کرد و البته نکات مهم دیگری هم وجود دارند که باید به آنها اشاره کرد. ممکن است مخاطبان گزارش ارزیابی همان افرادی نباشند که در تعیین محدوده ارزیابی نقش داشتند یا ممکن است حین اجرای ارزیابی عضوی از زنجیره ارتباطی نباشند. این مخاطبان می‌توانند طیف وسیعی داشته باشند از جمله کارمندان امنیت آگاه به مسائل فنی و مدیران ارشد کسب و کار محور؛ بنابراین گزارش باید به صورتی نوشته شود که همه مخاطبان توانایی درک یافته‌های آن را داشته باشند. پیش از پرداختن به یافته‌های ارزیابی، بهتر است که ابتدا خوانندگان گزارش (یا در رابطه با ارایه، شنوندگان آن) را با چگونگی، زمان، اجراکنندگان ارزیابی و آنچه مورد ارزیابی قرار گرفته آشنا کرد.

ممکن است مخاطبان در ابتدای ارزیابی چنین اطلاعاتی را نداشته باشند و در ارزیابی‌های طولانی‌تر هم یادآوری شرایط ارزیابی به درک بهتر و آشنایی با چارچوب نتایج کمک می‌کند.

باید بخشی از گزارش ارزیابی به ارایه توضیحاتی در رابطه با اجراکنندگان ارزیابی، آنچه که قرار بوده ارزیابی شود و مدت زمان اجرای ارزیابی اختصاص پیدا کند. ممکن است ارزیابی بسیار کوتاه و شامل محدوده‌ای کوچک باشد اما مدیر کسب و کار سازمان مشتری تا جلسه ارایه فصلی که توسط کارمندان امنیت سازمان انجام می‌شود نتایج را دریافت نکند. در صورتی که نتایج، مربوط به یک بازه زمانی کوتاه و محدوده‌ای خاص باشند، اگر این نکات مشخص نشده باشد ممکن است با توجه به نتایج ارزیابی این تصور ایجاد شود که ارزیابی ارزش هزینه صرف شده را نداشته است. باید در گزارش علاوه بر نشان دادن مشکلات امنیتی سازمان مشتری، برای پیگیری آنها هم انگیزه ایجاد کرد که این موضوع هم برای تیم‌های قرمز درون سازمانی و هم برای ارایه دهندگان خدمات امنیت تهاجمی اهمیت زیادی دارد. اگر نظر مدیر عملیاتی سازمان برای انجام فعالیت‌های ارزیابی جلب نشود، ممکن است بودجه تیم قرمز قطع شده و در نهایت منحل شده یا از تمدید قرارداد با آن خودداری شود. بدتر اینکه، ممکن است سازمان فعالیت‌های امنیت تهاجمی را به کلی رها کند و آنها را به چشم فعالیت‌های پرریسک و پرهزینه اتلاف کننده منابع ببیند.

پس از اینکه با مخاطبان در رابطه با عوامل شکل دهنده عملیات تیم قرمز گفتگو شد، بهتر است یک خلاصه کلی و سطح بالا از فعالیت ارزیابی در اختیار آنها قرار بگیرد. معمولاً من در این بخش از تعامل جزئیات مربوط به ترتیب انجام فعالیت‌ها را ذکر نمی‌کنم هر چند این اطلاعات هم می‌توانند مفید باشند. بررسی سطح بالای من شامل فعالیت‌های سرشماری و بهره برداری و همچنین نقاط حرکت مهم در ارزیابی است. می‌توان این روایت را در قالب فهرست نمونه زیر ارایه داد یا در قالب یک روایت آزادتر از ارزیابی.

- سازماندهی اطلاعات اپن سورس به دست آماده از فهرست اهداف خارجی
- اسکن پورت و بررسی دستی وب سایت میزبان‌های خارجی
- دسترسی اولیه به دست آمده با آسیب‌پذیری اجرای کد از راه دور در سایت
- سرشماری منطقه غیرنظامی (DMZ[1]) پس از دسترسی اولیه و شناسایی اهداف داخلی
- نفوذ به DMZ و فایل سرور داخلی برای حرکت هر چه بیشتر (در شبکه)
- سرشماری بیشتر ماشین‌های شناسایی شده در شبکه‌های داخلی

[1] demilitarized zone

- نفوذ به ماشین‌های کاربری که منجر به دسترسی به میزبان‌های مدیریتی (ادمین) می‌شوند
- نفوذ و بهره برداری از میزبان‌های مدیریتی برای دسترسی به کنترل‌گرهای دامنه
- نفوذ به کنترل‌گرهای دامنه و استفاده مجدد از اعتبارنامه‌های کاربری بین میزبان‌های لینوکسی و ویندوزی برای فراهم کردن امکان تکمیل نفوذ به سازمان

این خلاصه فعالیت‌های حمله، مهارت‌های ارزیاب را نشان داده و به خواننده کمک می‌کند تا یک درک فوری از شدت و اهمیت ارزیابی پیدا کند. همچنین چنین خلاصه‌هایی در مواقعی که ارزیابی موفقیت چندانی نداشته مفید هستند؛ می‌توان جزئیات بیشتری درباره نحوه اجرای فعالیت سرشماری در این گزارش‌ها درج کرد - حداقل برای نشان دادن کامل بودن تلاش‌های تیم ارزیابی. این اطلاعات باعث می‌شوند که مخاطب نسبت به تلاش‌های ارزیاب دید بهتری پیدا کرده و این واقعیت برای مخاطب یادآوری شود که مختصر بودن نتایج ناشی از خوب بودن وضعیت امنیتی سازمان است نه اجرای بد ارزیابی توسط تیم قرمز و به این ترتیب مخاطب را برای گزارش مختصرتر آماده می‌کنند.

آخرین نکته‌ای که باید پیش از پرداختن به خود یافته‌ها به آن اشاره کنیم، پرداختن به هر گونه بی‌نظمی شناسایی شده حین ارزیابی است. این گزارش فرصت خوبی برای اشاره به موارد مشکوک شناسایی شده در شبکه است که از نظر تیم ارزیابی باید به آنها اشاره شود اما جزء یافته‌های امنیتی که باید به آنها رسیدگی شود نیستند مثل شناسایی دستگاه‌ها، سرویس‌ها یا ترافیک غیرمنتظره درون سازمان. به عنوان مثال می‌توان به پیدا کردن یک تلفن همراه در شبکه اشاره کرد یا شناسایی یک سیستم ویندوزی خارج از دامنه و سایر اکتشافاتی که لزوماً تهدیدی برای سازمان نیستند اما خوب است به آنها اشاره شود چون از نظر تیم ارزیابی، غیرعادی یا ناهنجار به نظر می‌رسند.

همچنین باید تیم ارزیابی در این بخش از گزارش به شناسایی فعالیت‌های مخرب یا غیرقانونی در سازمان حین اجرای ارزیابی اشاره کند. گرچه باید این اطلاعات از قبل و به محض شناسایی فعالیت مخرب حین ارزیابی در اختیار سازمان قرار گرفته باشد اما خوب است که دوباره به آن اشاره شود چون ممکن است فراموش شده یا کنار گذاشته شده باشد و شناسایی این تهدیدات نشان دهنده تلاش و کوشش تیم ارزیابی است. در نهایت، تیم قرمز می‌تواند در این بخش به فعالیت‌های غیرعادی کارمندان امنیت سازمان که نشان دهنده اقدام ناشایست از طرف پرسنل امنیتی بوده، برای تیم قرمز مانع ایجاد کرده و باعث اتلاف منابع شده‌اند، اشاره کند. این اکتشافات

می‌توانند شامل شناسایی پیکربندی‌های خاصی در نرم‌افزار امنیتی یا گزارش وقایعی باشند که نشان دهنده هدف گرفتن فعالیت‌ها یا ابزارهای تیم قرمز هستند یا وجود اسکریپت و ابزارهای دیگری که قصد شکار تیم قرمز را نشان می‌دهند. همانطور که در ابتدای این کتاب اشاره شد، چنین فعالیت‌هایی برای سازمان مضر هستند و ممکن است بهتر باشد این یافته‌ها در گزارش مطرح شوند. همچنین در شرایطی که نتیجه‌ای وجود ندارد یا وقتی کارمندان امنیتی پس از گیر انداختن تیم قرمز یافته‌های آنها را زیر سوال می‌برند، مطرح کردن این نکات می‌تواند برای ارتقای وضعیت امنیتی سازمان و حفظ اعتبار کلی تیم ارزیابی مفید باشد.

اما پیش از انجام این کار به خصوص در صورتی که تیم قرمز برون سازمانی است، برای اشاره به چنین فعالیت‌هایی در گزارش بسیار محتاط باشید چون ممکن است باعث تیره شدن هر چه بیشتر روابط شود. برای مثال، ممکن است کارمندان امنیت یک امضاء برای باینری خاص تیم قرمز نوشته باشند یا آی‌پی‌های تیم قرمز را به دست آورده باشند. در این صورت، می‌توان در گزارش از چنین جملاتی استفاده کرد "گرچه تیم امنیت توانست با این پیاده سازی مانع از فعالیت ما شود اما مایل هستیم که به آنها برای مقابله با مهاجمان کمک کنیم، نه فقط فعالیت تیم قرمز چون این کار کمک بیشتری به بهبود وضعیت امنیت سازمان می‌کند." با این طرز بیان می‌توانید همزمان با اشاره به اینکه کارمندان امنیت مانع تلاش‌های شما شده‌اند، به آنها برای مقابله با مهاجمانی که از تکنیک‌های مشابه استفاده می‌کنند، پیشنهاد کمک بدهید. بهتر است با گزارش، ذهن و قلب مخاطب را به خود جلب کنید و از آن به عنوان فرصتی برای توبیخ و سرزنش استفاده نکنید.

انواع یافته‌ها

در این بخش به بررسی اصلی گزارش می‌پردازیم که شامل خود یافته‌ها و بهترین راه انتقال آنها به مشتری است. یافته‌ها انواع مختلفی دارند و می‌توان این موضوع را در شیوه ترسیم و انتقال یافته‌ها به مشتری منعکس کرد. بدیهی‌ترین یافته، وجود یک آسیب‌پذیری در یکی از نرم‌افزارهای نصب شده است که تیم ارزیابی از آن برای دستکاری یا تأثیرگذاشتن بر هدف استفاده کرده است. اما خیلی از یافته‌ها چنین ماهیت فنی ندارند و ممکن است مربوط به پیکربندی‌های اشتباه یا نبود پیکربندهایی باشند که منجر به اجرای موفقیت آمیز حمله شده‌اند. بسیاری از مواقع، اثبات مفهوم یک آسیب‌پذیری از طریق بهره برداری موفق از آن کار نامناسبی است بنابراین اعلام اینکه چنین یافته‌هایی وجود داشته‌اند اما از آنها بهره برداری نشده، باز هم برای مشتری

بسیار مفید است. یافته‌هایی که ماهیت فنی کمتری دارند مثل فقدان پیاده سازی‌های رویه‌ای یا سیاست‌هایی خاص هم می‌توانند امکان نفوذ به بخش‌هایی از سازمان را برای ارزیاب‌ها فراهم کنند.

آسیب‌پذیری‌های بهره‌برداری شده

همانطور که اشاره شد، آسیب‌پذیری‌های بهره برداری شده به آسیب‌پذیری‌های شناسایی شده‌ای گفته می‌شود که بر علیه سازمان از آنها استفاده شده است. انجام این کار لزوماً همیشه ضروری نیست و ممکن است در برخی از تعاملات نیاز به بهره برداری وجود نداشته باشد یا کم باشد. در واقع، نفوذ به سیستم راه خوبی برای نشان دادن خطر آسیب‌پذیری است. معمولاً خطرناک‌ترین بخش از نفوذ به یک سیستم، وجود آسیب‌پذیری نیست بلکه دسترسی‌هایی است که پس از آن ایجاد می‌شود یا داده‌هایی که افشا می‌شود. مهم است که در چنین یافته‌هایی برای توضیح نحوه بهره برداری از موفقیت آمیز از آسیب‌پذیری، صداقت را رعایت کرد. این کار به کارمندان امنیتی امکان می‌دهد که خطر آسیب‌پذیری را بهتر درک کنند و ممکن است با در اختیار داشتن این اطلاعات برای رسیدگی به آسیب‌پذیری روش متفاوتی را انتخاب کنند.

ممکن است آسیب‌پذیری‌های بهره برداری شده شامل کارهایی باشند که ارزیاب و مشتری هر دو باید انجام دهند و مجزا از سایر یافته‌ها هستند. این شرایط خاص وقتی ایجاد می‌شود که تیم قرمز یک آسیب‌پذیری قبلاً فاش شده را شناسایی می‌کند یا یکی از آسیب‌پذیری‌هایی که قبلاً مورد بهره برداری قرار گرفته اما شناسایی شده را مسلح سازی می‌کند. اگر این آسیب‌پذیری یا اکسپلویت در نرم‌افزاری شناسایی شود که متعلق به سازمان مشتری نیست، احتمالاً مشتری در رابطه با آنچه با این آسیب‌پذیری انجام می‌شود، کنترل و نفوذ زیادی ندارد. اما تیم ارزیابی باید درباره اینکه این آسیب‌پذیری را چطور به اطلاع عموم و توسعه دهنده اپلیکیشن می‌رساند، آگاهانه تصمیم گیری کند. ممکن است تیم قرمز در این مرحله جزئیات آسیب‌پذیری را فاش کند اما همزمان که تیم در تلاش برای شناسایی بهترین راه انتشار اطلاعات آسیب‌پذیری است، یک توافقنامه عدم افشا با سازمان مشتری امضا کند. بعلاوه، گاهی اوقات ممکن است نرم‌افزار مورد بهره برداری در اصل متعلق به سازمان مشتری و بخشی از مدل کسب و کار آن باشد. در چنین شرایطی ممکن است مشتری مایل باشد که این فرایند افشا (یا به احتمال، پیشگیری از افشای این اطلاعات) توسط خود مشتری هدایت شده و از تیم ارزیابی بخواهد که برای پیشگیری از افشای آسیب‌پذیری، یک توافقنامه عدم افشا امضا کند. در هر صورت، شناسایی و مسلح سازی آسیب‌پذیری توسط هکرهای اخلاقی برای اولین بار نقش مهمی در ارتقای شهرت و رزومه کاری

آنها دارد به ویژه در صورت درج آن در پایگاه داده ملی آسیب‌پذیری‌ها که تحت مدیریت مؤسسه ملی استانداردها و فناوری [آمریکا] قرار دارد.

آسیب‌پذیری‌های بهره‌برداری نشده

به دلایل مختلف ممکن است یک آسیب‌پذیری در یک سیستم شناسایی شود اما ارزیاب یا حتی مشتری از بهره برداری آن برای اثبات مفهوم خودداری کند. مثلاً اگر آسیب‌پذیری در بخش زیادی از سازمان وجود داشته باشد، لازم نیست که پس از هر بار شناسایی آن روی هر ماشین برای نشان دادن ریسک حضور آن در سازمان، با موفقیت از آن بهره برداری کرد. در واقع اگر تیم ارزیابی سعی کنند بارها از یک آسیب‌پذیری روی سیستم‌های مختلف بهره برداری کنند بدون اینکه این کار را به صورت هدفمند و گزینشی انجام دهند، این اقدام بی‌احتیاطی محسوب می‌شود. به همین ترتیب، ممکن است از طریق یک آسیب‌پذیری امکان نفوذ به یک سیستم فراهم شود اما پس از نفوذ با بررسی بیشتر هدف مشخص شود که چند آسیب‌پذیری اجرای کد از راه دور دیگر در چندین نرم‌افزار نصب شده روی سیستم وجود دارد. در چنین شرایطی، با توجه به اینکه تیم ارزیابی از قبل به این سیستم نفوذ کرده است، نیازی به اثبات مفهوم آسیب‌پذیری‌های دیگر نیست.

همچنین ممکن است مشتری متوجه شود که انجام چنین فعالیتی خطر زیادی به همراه دارد و از تیم ارزیابی درخواست کند که دستگاه یا اپلیکیشن را رها کرده یا دسترسی را به روش‌هایی امن‌تر فراهم کنند تا امکان ادامه ارزیابی وجود داشته باشد. در مجموع خوب است برای بهره برداری از یک آسیب‌پذیری از این استدلال استفاده کنیم که اگر بهره برداری از آسیب‌پذیری به نفوذ هر چه بیشتر در سازمان یا نشان دادن جدیت یک آسیب‌پذیری خاص کمکی نمی‌کند، احتمالاً ریسک استفاده از آن بیشتر از سود و منفعت این کار خواهد بود. اگر به یک مشتری اعلام کنیم که روی بیشتر سیستم‌های ویندوزی سازمان آنها آسیب‌پذیری MS17-010 پیدا شده و می‌توانیم با استفاده از این آسیب‌پذیری به سیستم‌های سازمان دسترسی پیدا کنیم، قطعاً جدیت گفتار ما به اندازه‌ای هست که توجه مشتری را به این واقعیت جلب کند و احتمالاً درخواست دسترسی سطح سیستمی به چند ماشین برای شبیه سازی بهره برداری نسبت به احتمال دیده شدن خطای "صفحه آبی" روی سیستم‌های شبکه، رویکرد حرفه‌ای‌تری خواهد بود.

آسیب‌پذیری‌های فنی

آسیب‌پذیری‌های فنی به آسیب‌پذیری‌های موجود در سیستم عامل‌ها یا اپلیکیشن‌ها گفته می‌شود که ناشی از به کار بردن روش‌های توسعه ضعیف یا ارتقای روش‌های بهره برداری هستند.

تفکیک انواع آسیب‌پذیری‌ها اهمیت زیادی دارد چون احتمالاً خود سازمان مقصر وجود این آسیب‌پذیری‌ها نیست. هنگام بررسی و توضیح این موضوع در گزارش یا ارایه، توجه به نکاتی مثل اینکه آسیب‌پذیری اجرای کد از راه دور که در یکی از نرم‌افزارهای سازمان شناسایی شده، همین یک هفته پیش به صورت عمومی معرفی شده، ضروری است. در مقابل، وقتی سازمان از نرم‌افزاری استفاده می‌کند که سال‌ها از شناسایی و معرفی آسیب‌پذیری‌های آن می‌گذرد، باید برخورد متفاوتی داشت و احتمالاً در این حالت به اقداماتی فراتر از نصب جدیدترین و امن‌ترین نسخه نرم‌افزار نیاز خواهد بود. در چنین شرایطی احتمالاً یافته‌های مجزایی درباره مدیریت وصله‌های امنیتی، جامعیت پیکربندی سیستم‌ها یا مسائل دیگر وجود خواهد داشت.

آسیب‌پذیری‌های غیرفنی

گروه بعدی آسیب‌پذیری‌ها، شامل مواردی هستند که به وجود یک نقص در کد ارتباط ندارند. این آسیب‌پذیری‌ها می‌توانند شامل مواردی مثل پیکربندی غلط یک دستگاه، عدم پیکربندی یک دستگاه (مثل استفاده از رمزهای پیش فرض) یا حتی نبود یک سیاست یا رویه مشخص باشند. این آسیب‌پذیری‌ها هم می‌توانند به همان میزان جدی و تأثیرگذار باشند چون احتمالاً فقط بر دستگاه یا دستگاه‌هایی که یک آسیب‌پذیری خاص دارند، تأثیرگذار نیستند. نبود رویه‌هایی مثل مدیریت وصله‌های امنیتی جزء یافته‌های تأثیرگذار بر کل سازمان هستند و باید آنها را جدی‌تر از کدهای آسیب‌پذیری که وجودشان ناشی از همین نقص است، دانست. یک عملیات خوب می‌تواند یافته‌هایی با چنین ماهیتی داشته باشد که مربوط به پیاده سازی ضعیف سیاست‌ها یا فقدان سیاست‌های لازم هستند. اگر حین ارزیابی، کارمندان امنیت سازمان با وجود شناسایی فعالیت‌های تیم قرمز، رویه‌های واکنش به حادثه را رعایت یا اجرا نکنند، این بی‌توجهی نشان دهنده وجود یک آسیب‌پذیری غیرفنی و بسیار مهم در وضعیت امنیت سازمان است.

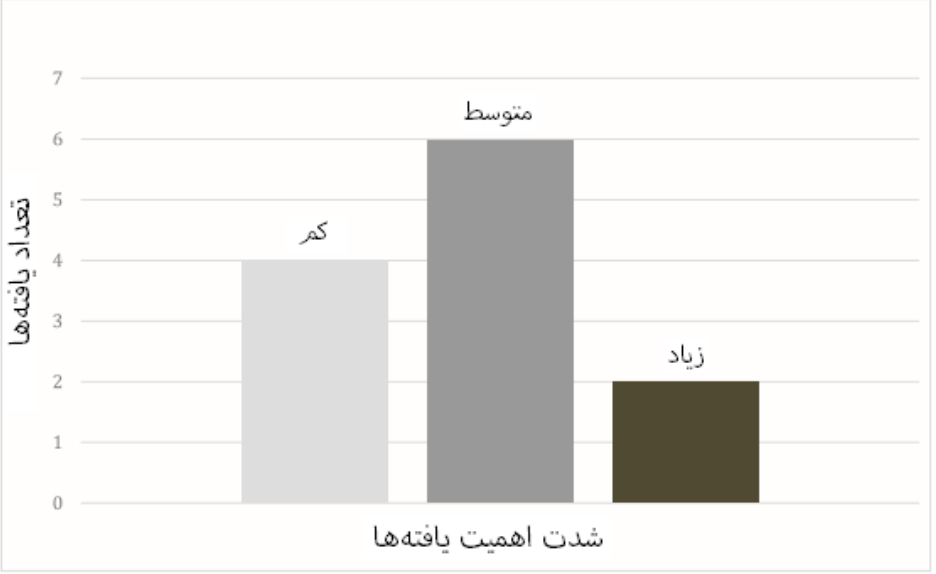
ثبت یافته‌ها

پس از بررسی انواع یافته‌ها در یک ارزیابی، در این قسمت به مرور روش‌های مناسب ثبت یافته‌ها در گزارش می‌پردازیم. پس از اطلاع رسانی به مشتری درباره آنچه در سازمان پیدا شده، نکته مهم بعدی مشخص کردن شدت وخامت و جدیت این آسیب‌پذیری‌ها است. اگر میزان اهمیت یافته‌ها نسبت به یکدیگر برای مخاطبان گزارش مشخص نباشد، هنگام انتخاب استراتژی مناسب جهت رفع آسیب‌پذیری هم با چالش روبرو خواهند شد. همچنین این گزارش نقش مهمی در تحلیل هزینه-فایده برای سازمان دارد. اگر مشتری نتواند به راحتی تصمیم بگیرد که اول کدام

آسیب‌پذیری‌ها را رفع کند، کدام آسیب‌پذیری‌ها باید رفع شوند و کدام را می‌توان پذیرفت، حتی اگر جزئیات آسیب‌پذیری‌ها به خوبی مشخص شده باشد، گزارش تهیه شده فایده چندانی نخواهد داشت.

خلاصه یافته‌ها

در بسیاری از گزارش‌ها پیش از پرداختن به هر یافته به صورت اختصاصی، یک خلاصه از یافته‌ها درج می‌شود. می‌توان این کار را با استفاده از یک نمودار میله‌ای ساده انجام داد که در یک نگاه تعداد آسیب‌پذیری‌های موجود و شدت آنها را نشان می‌دهد (شکل ۷-۱).

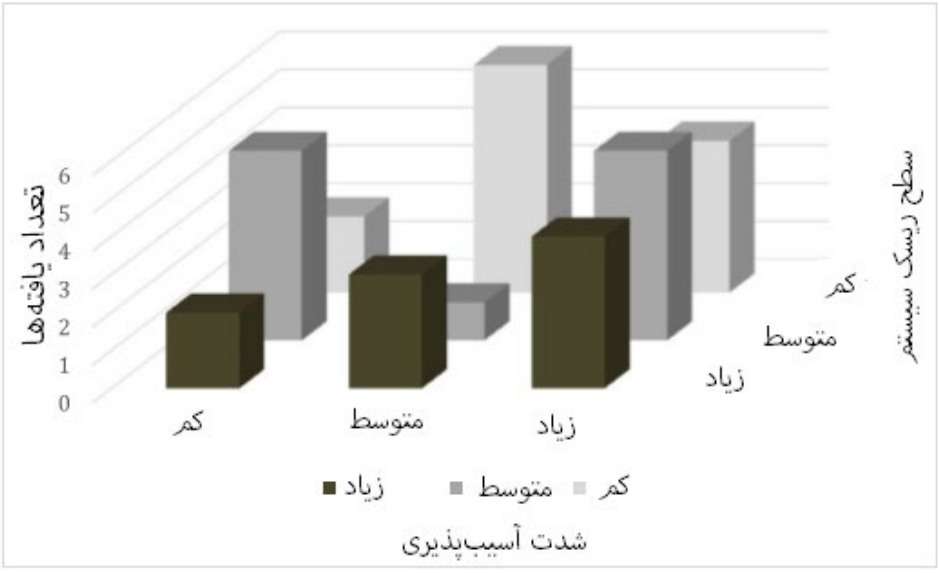


شکل ۷-۱ شدت وخامت یافته‌ها

این نمودار، روشی ساده و آسان برای مشخص کردن تعداد آسیب‌پذیری‌های شناسایی شده و میزان جدیت آنها است. یکی از مشکلات این نمودار این است که معمولاً شدت آسیب‌پذیری بر اساس میزان خطرناک بودن آن یافته خاص برای سیستمی که آسیب‌پذیری روی آن پیدا شده مشخص می‌شود نه لزوماً میزان خطری که یک یافته خاص برای سازمان دارد. یک روش بهتر برای خلاصه کردن یافته‌ها، مشخص کردن خطر آسیب‌پذیری برای سیستمی که آسیب‌پذیری روی آن پیدا شده و خطر نفوذ به آن سیستم برای کل سازمان است. ممکن است آسیب‌پذیری اجرای کد از راه دور برای یک سیستم خطرناک باشد اما وجود این آسیب‌پذیری روی دستگاهی که برای

دسترسی مهمانان به اینترنت در لابی سازمان قرار گرفته و به دستگاه‌های دیگر متصل نیست، تهدید چشمگیری برای وضعیت امنیتی کلی سازمان نیست. از منظر هزینه-مزایا صرف منابع برای رفع این آسیب‌پذیری "شدید" روی یک سیستم بی‌اهمیت اقدام ضعیفی خواهد بود.

اما چطور باید به مشتری برای اولویت بندی رسیدگی به آسیب‌پذیری‌ها کمک کنیم؟ طبق تجربه من، یکی از بهترین روش‌های انجام این کار تهیه فهرستی از میزبان‌هایی است که هیچ یافته‌هایی در آنها وجود نداشته و بعد از مشتری درخواست شود که با فرض نفوذ، ریسک آنها را رده بندی کند. سپس ارزیاب با در نظر گرفتن این داده‌ها و یافته‌های قبلی نموداری شبیه به شکل ۷-۲ ایجاد می‌کند که شدت اهمیت آسیب‌پذیری‌ها را به همراه اهمیت سیستم‌های آسیب‌پذیر برای سازمان مشخص می‌کند.



شکل ۷-۲ سیستم‌های بحرانی یافته‌ها

با استفاده از نمودار شکل ۷-۲ مخاطبان می‌توانند ریسک واقعی یافته‌ها را از هم تفکیک کنند و طیف آنها را از گوشه سمت چپ بالا (که نشان دهنده یافته‌های کم ریسک روی سیستم‌های کم ریسک هستند) تا گوشه سمت راست پایین (که مربوط به یافته‌هایی با ریسک بالا روی سیستم‌های پرریسک هستند) تشخیص دهند. این نمودار به همراه داده‌های مربوط به هر یافته،

به تیم ارزیابی امکان می‌دهد که سازمان مشتری را برای تدوین استراتژی مقابله با تهدید به بهترین شکل هدایت کنند.

نمایش یافته‌ها به صورت مجزا

اما پس از ارایه خلاصه، بهترین راه نمایش یافته‌ها به صورت مجزا در گزارش چیست؟ من به شخصه یافته‌ها را از بیشترین تأثیر تا کمترین تأثیر مرتب کرده و اطلاعاتی مثل آنچه در ادامه ارایه شده را برای هر یافته درج می‌کنم.

یافته ۱: آسیب‌پذیری‌های نسخه 9.0.0.29935 از Foxit Reader

شدت: زیاد

آسیب‌پذیری‌ها:

CVE-2018-9979 افشای اطلاعات

	محرمانگی	جامعیت	دسترس پذیری
ریسک	متوسط	کم	کم

CVE-2018-9981 اجرای کد از راه دور

	محرمانگی	جامعیت	دسترس پذیری
ریسک	زیاد	زیاد	زیاد

فعالیتی که به شناسایی کمک کرده است: سرشماری و حمله به شبکه داخلی

سیستم‌هایی که آسیب‌پذیری در آنها پیدا شده است:

سیستم	سطح ریسک برای سازمان
192.168.97.44	کم
192.168.97.47	کم
192.168.97.90	متوسط
192.168.97.91	متوسط
192.168.97.201	زیاد

توضیحات مفصل یافته‌ها: حین اجرای عملیات، نسخه نصب شده Foxit Reader امکان اجرای کد از را دور را روی چند سیستم سازمان فراهم کرد. اجرای یک اسکن روی شبکه برای بررسی

وجود این آسیب‌پذیری روی سایر سیستم‌ها، نشان داد که این آسیب‌پذیری در چند میزبان دیگر هم حضور دارد. اجرای بهره برداری اثبات مفهوم روی همه میزبان‌ها ضروری به نظر نمی‌رسید.

کاهش یا اصلاح: نصب جدیدترین نسخه از نرم‌افزار **Foxit Reader** به کاهش این تهدیدات کمک می‌کند.

در اینجا نکات زیادی را مطرح می‌کنیم طوری که درک آنها راحت باشد و به مخاطب برای هضم یافته‌های مختلف و جزئیات آنها کمک کند. در ابتدا خود یافته را پوشش می‌دهیم که در اینجا، استفاده از یک نسخه قدیمی و به روز نشده از **Foxit Reader** است. سپس شدت وخامت کلی یافته‌ها را به همراه آسیب‌پذیری مورد استفاده برای آنها مشخص می‌کنیم. لزوماً در همه یافته‌ها چندین آسیب‌پذیری وجود ندارد و در این مورد این نسخه خاص از **Foxit** ده‌ها آسیب‌پذیری دارد اما برای توضیحات فقط دو مورد از آنها را ذکر کردیم. آسیب‌پذیری اول **CVE-2018-9979** است. **CVE**[2] مخفف آسیب‌پذیری‌ها و مواجهه‌های مشترک است که یک فهرست آسیب‌پذیری است و شرکت **Mitre** آن را به عنوان سندی عمومی مدیریت و نگهداری می‌کند. **CVE-2018-9979** یک آسیب‌پذیری افشای اطلاعات در این نسخه از **Foxit** است و ممکن است مهاجمان با استفاده از آن بتوانند بدون احرازهویت و مجوز به اطلاعات سیستم دسترسی پیدا کنند. این آسیب‌پذیری هم جدی است اما نه به اندازه آسیب‌پذیری بعدی - **CVE2018- 9981** - که امکان اجرای کد از راه دور را فراهم می‌کند.

پس از مشخص کردن اطلاعات فنی، نوع فعالیتی که منجر به شناسایی و یا بهره برداری از آسیب‌پذیری شده است را مشخص می‌کنم چون این اطلاعات می‌توانند به اصلاح یا کاهش تهدید کمک کنند. بعد از آن توضیح می‌دهیم که آسیب‌پذیری در کدام سیستم‌ها وجود داد. در یافته ۱، خطری را که توسط خود سیستم‌ها برای سازمان ایجاد شده هم توضیح داده‌ایم. این اطلاعات باید از سازمان مشتری به دست بیایند و همیشه لزوماً هنگام ایجاد گزارش در دسترس شما نیستند. از آنجایی که با کمک این اطلاعات می‌توان سطح ریسک را به بهترین شکل ممکن نشان داد، باید هر زمان ممکن بود این اطلاعات را ارایه داد. پس از مشخص کردن سیستم‌های آسیب‌پذیر، جزئیات یافته‌ها و نحوه استفاده و بهره برداری از آنها را توضیح می‌دهیم - این کار هم برای کمک به رفع آسیب‌پذیری‌ها انجام می‌شود. در نهایت، راهنمای رفع یا اصلاح آسیب‌پذیری را در اختیار مشتری قرار می‌دهیم. برخی از مشتری‌ها تمایلی به دریافت این اطلاعات

[2] common vulnerabilities and exposures

ندارند اما به نظر من بهتر است برای اصلاح آسیب‌پذیری‌ها هم طرز فکر امنیت تهاجمی را در نظر داشت حتی اگر در نهایت کارمندان بخش امنیت سازمان مشتری از این اطلاعات استفاده نکنند.

در ادامه مثالی از یک آسیب‌پذیری مشاهده می‌کنید که در کد یکی از اپلیکیشن‌های نصب شده پیدا نشده است. این آسیب‌پذیری هم جنبه فنی و هم جنبه غیرفنی دارد.

یافته ۲: نبود سیاستی برای انقضای رمزهای عبور

شدت: کم

آسیب‌پذیری‌ها: به دلیل پیکربندی خاص سیستم، رمزهای عبور منقضی نمی‌شوند و هیچ سیاستی در این زمینه وجود ندارد.

	محرمانگی	جامعیت	دسترس پذیری
ریسک	کم	کم	کم

فعالیتی که به شناسایی کمک کرده است: سرشماری و حمله به شبکه داخلی

سیستم‌هایی که آسیب‌پذیری در آنها پیدا شده است:

سیستم	سطح ریسک برای سازمان
192.168.97.44	کم
192.168.97.47	کم
192.168.97.90	متوسط
192.168.97.91	متوسط
192.168.97.201	زیاد

توضیحات مفصل یافته‌ها: پس از دسترسی به چندین میزبان، مشخص شد که سیاست انقضای رمزعبور روی این سیستم‌ها پیاده سازی نشده است. همچنین پس از گفتگو با کارمندان بخش امنیت سازمان، مشخص شد که سیاستی در این زمینه وجود ندارد.

کاهش یا اصلاح: اعمال سیاست‌های انقضای رمزعبور در سطح سیاست‌ها، سیستم‌ها و برنامه‌های کاربردی.

سپس هر آنچه تا اینجا در این گزارش توضیح داده شده را در قالب یک استراتژی کاهش ریسک خلاصه می‌کنیم. این استراتژی می‌تواند شبیه به جدول زیر باشد که ترتیب کارها را برای سازمان مشخص می‌کند تا برای اصلاح و رفع تهدیدات به موارد مهم‌تر اولویت دهد. ممکن است

سازمان، محدودیت‌های عملیاتی دیگری هم داشته باشد، یا برای سازمان قابل قبول باشد که برخی موارد را به جای اصلاح مدیریت کند و غیره. اما بهترین راه نشان دادن نقشه راه رفع ریسک توسط تیم ارزیابی، همین روش است:

اولویت	سیستم	ریسک برای سازمان	یافته	ریسک
1	192.168.97.200	زیاد	1	زیاد
2	192.168.90	متوسط	1	زیاد
3	192.168.90	متوسط	1	زیاد
4	192.168.97.200	زیاد	2	کم
5	192.168.91	متوسط	2	کم
6	192.168.91	متوسط	2	کم
7	192.168.97.44	کم	1	زیاد
8	192.168.97.47	کم	1	زیاد
9	192.168.97.44	کم	2	کم
10	192.168.97.47	کم	2	کم

ارایه

به نظر من، مؤثرترین نتایج ارزیابی آنهایی هستند که با یک گزارش خوب به مخاطبان منتقل شده و با یک ارایه خوب از آنها حمایت می‌شود. همیشه ارایه به صورت حضوری ممکن نیست چون برخی از تعاملات تیم قرمز از راه دور انجام می‌شوند اما بهتر است پس از تحویل گزارش به سازمان مشتری، یک ارایه توسط تیم ارزیابی انجام شود. این ارایه نباید تکرار آنچه در گزارش بیان شده باشد بلکه باید حاوی اطلاعات مکملی باشد که اهمیت نتایج و همچنین اهمیت ارزیابی امنیت تهاجمی را نشان می‌دهند. روش پیشنهادی من، تهیه چند اسلاید با یک نقشه سطح بالا از شبکه سازمان است که هر اسلاید گام مهمی از مراحل نفوذ به سازمان باشد - مثل لیستی که برای خلاصه فعالیت‌ها تهیه شده بود.

حین اجرای ارایه، ارزیاب مراحل نفوذ را برای مخاطبان شرح داده و خلاصه‌ها و اهداف ساده گزارش را تبدیل به یک ارایه قابل درک می‌کند طوری که حتی کارمندان غیرفنی هم اهمیت همه

یافته‌ها را درک کنند حتی یافته‌هایی با شدت وخامت کمتر. نشان دادن اینکه چطور یک یافته کوچک منجر به رسیدن به یافته‌ای دیگر شده و این زنجیره تا زمان نفوذ به زیرساخت سازمان و امکانات مدیریتی آن ادامه پیدا کرده نه تنها برای مخاطبان آموزنده است بلکه اهمیت کار ارزیاب و کل فعالیت‌های تیم قرمز را نشان می‌دهد. تیم قرمز با چنین ارایه‌ای می‌تواند به مخاطبان نشان دهد که نفوذ توسط یک مهاجم مخرب به چه صورت است. سرشماری مهاجم، مسئولیت تیم قرمز است و به تصویر کشیدن چرخه عملکرد مهاجم به شکل مؤثر، بیشترین درک ممکن را نسبت به وضعیت امنیت سازمان و آنچه مستلزم رسیدگی و توجه است، فراهم می‌کند.

ارزیابی بدون نتیجه

آخرین نکته‌ای که در رابطه با گزارش دهی باید به آن بپردازیم، ارزیابی‌های بدون نتیجه است - یا ارزیابی‌هایی بدون نتیجه قابل توجه. تیم ارزیابی و مشتری باید درک کنند این که هیچ دستگاهی با موفقیت مورد نفوذ قرار نگرفته، به معنای شکست خوردن ارزیابی نیست. پیش از این هم به چنین تصورات اشتباهی در رابطه با نخبه گرایی در هک و نیاز به دیدن شدن به عنوان یک هکر نخبه اشاره کرده بودیم. باز هم به شما و به مشتری یادآوری می‌کنیم که هدف تیم‌های قرمز حرفه‌ای، تقویت وضعیت امنیتی یک سازمان است نه نفوذ به یک دستگاه، اپلیکیشن یا نرم‌افزار. نفوذ تنها یک راه برای رسیدن به یک هدف است نه هدف نهایی یا تنها مسیر برای رسیدن به آن. اگر هیچ نتیجه چشمگیری در هیچ ارزیابی وجود ندارد، باز هم توصیه‌های ما در رابطه با گزارش پابرجا هستند. به جای تمرکز بر اینکه ارزیابی چه کاستی‌هایی داشته، متمرکز بر این شوید که چه ارزیابی‌هایی انجام شده است. با این کار، حداقل دستگاه امنیت سازمان متوجه می‌شود که کدام بخش‌ها وضعیت خوبی دارند و کدام بخش‌ها احتمالاً مورد ارزیابی قرار نگرفته‌اند و بهتر است در ارزیابی‌های داخلی به آنها توجه داشت.

بعلاوه، اگر شرایط تعیین شده برای ارزیابی بیش از حد محدود کننده بوده و تأثیر نامطلوبی بر تعاملات دارند، باید این موضوع را هم انتقال داد. گزارش دهی برای چنین تعاملی باید به بیشترین میزان ممکن مشتری را برای پیاده سازی ارزیابی بعدی راهنمایی کند. تیم ارزیابی می‌تواند به نکاتی مثل این اشاره کند که بازه زمانی در نظر گرفته شده برای این تعامل کوتاه بوده یا محدوده تعیین شده به خوبی کل سطوح حمله مربوطه را پوشش نداده یا اینکه تیم می‌تواند با بهره برداری‌های اثبات مفهوم بیشتر یا نفوذ و انتقال به سیستم‌های بعدی، اطلاعات بیشتری در رابطه با مشکلات امنیتی سازمان فراهم کند. ارزیاب و مشتری باید همه تلاش خودشان را

برای موفقیت ارزیابی و رسیدن به سطح خوبی از هزینه-منافع در رابطه با کاهش تهدیدات انجام دهند. اما، لزوماً همیشه نتیجه به این صورت نیست و ممکن است کم بودن یا فقدان نتایج، اولین گام برای شروع یک ارزیابی جامع‌تر از طریق انتخاب یک محدوده، زمانبندی، **ROE** و اجرای مناسب‌تر این فعالیت باشد.

خلاصه فصل هفتم

در این فصل به بررسی اهمیت گزارش دهی پرداخته، راه‌های مناسب برای ثبت محتوای یک گزارش را توصیه کرده و در نهایت به بررسی برخی از روش‌های مطلوب برای ارایه گزارش پرداختیم.

• 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.