Microsoft Enterprise Cloud
Red Teaming

Naserifard.aidin@gmail.com

Aidin-naserifard

مترجم: **آیدین ناصری فرد**

تابستان ۱۳۹۶

چکیده

در این مقاله در مورد استراتژی مایکروسافت و اجرای Red Teaming و همچنین آزمون نفوذ بر روی زیرساخت مدیریت شده ابر مایکروسافت، سرویس‌ها و برنامه‌های کاربردی بحث خواهد شد. شما خواهید آموخت که مایکروسافت چگونه یک نمونه مشابه دنیای واقعی را شبیه‌سازی می‌کند و همچنین نظارت‌های مداوم امنیتی و اقدامات پاسخگویی به حوادث امنیتی برای اعتبارسنجی و بهبود امنیت محصولات Microsoft Azure و Office 365 چگونه انجام می‌گیرد. علاوه بر این شما را با رویکرد امنی که مشتریان باید در هنگام نصب و مدیریت دارایی‌های مبتنی بر ابر داشته باشند، آشنا می‌کند. Red Teaming چیزی بیشتر از رعایت اعتبارنامه‌ها[1] و سایر نیازهای صنعت است و برای مایکروسافت و مشتریان آن تضمین‌های اضافی خدمات ابر مایکروسافت شامل نظارت امنیتی، آزمون نفوذ و به‌روزرسانی‌ها برای تهدیداتی که با آن‌ها مواجه می‌شوند را به‌طور مداوم فراهم می‌کند.

اطلاعات بیشتر

آزمون نفوذ در مقیاس سازمانی نیاز به درگیر شدن چندین شرکت در سازمان دارد. این سند راهنمای فرآیندی برای افرادی که مسئول ارزیابی محیط‌ها، سیستم‌ها و فرایندها برای تهدیدات امنیتی هستند، می‌باشد. باید توجه داشت که جزئیات ارائه شده در اینجا یک مرور کلی بر چگونگی آزمون نفوذ تیم‌های امنیتی Microsoft Azure و Office 365 توسط Red Teaming و آزمون نفوذ لحظه‌ای سیستم است و دستورالعمل‌های چگونگی حمله مشتریان به زیرساخت‌های ابر، پلتفرم‌ها یا سرویس‌های مایکروسافت را شامل نمی‌شود. در حالی که مایکروسافت به‌طور منظم آزمون نفوذ را برای بهبود کنترل و پردازش‌های امنیتی ابر خود انجام می‌دهد، ما متوجه خواهیم شد که ارزیابی‌های امنیتی بخش مهمی از فعالیت‌های توسعه برنامه‌های مشتریان خواهد بود. بنابراین ما سیاستی را ایجاد نموده‌ایم که مشتریان بتوانند آزمون‌های نفوذ مجاز را در برنامه‌های خود که بر روی Microsoft Azure میزبانی می‌شوند، انجام دهند. از آنجا که این آزمون‌ها قابل تشخیص از حملات واقعی نیستند، باید تنها پس از اخذ تأییدیه از تیم پشتیبانی مشتریان مایکروسافت صورت پذیرد. آزمون نفوذ باید مطابق شرایط و ضوابط تیم مایکروسافت انجام شود. برای اطلاعات بیشتر در این زمینه می‌توان به لینک زیر مراجعه نمود:

http://azure.microsoft.com/en-us/support/trust-center/security/

[1] Compliance Accreditations

فهرست

۱ . مقدمه

سازمان‌ها می‌توانند با شبیه‌سازی حملات دنیای واقعی و اِعمال ترفندها، تکنیک‌ها و روش‌ها که معمولاً مهاجمان از آن‌ها بهره می‌برند، خود را برای حملات واقعی آماده سازند. به‌جای آنکه سعی در جلوگیری از وقوع حوادث امنیتی داشت، بسیار مهم است که تصور نمود که این حوادث امنیتی می‌توانند رخ دهند و در آینده نیز اتفاق خواهند افتاد. اطلاعات به‌دست‌آمده از Red Teaming و تمرینات آزمون نفوذ آنلاین بر روی سایت‌ها، کمک می‌کند تا به‌طور قابل‌توجهی دفاع در برابر حملات تقویت شده، استراتژی‌های واکنش به حملات و آموزش دفاعی در برابر حملات بهبود یابد و کارایی کل طرح امنیتی تداوم داشته باشد.

سازمان‌ها نمی‌توانند به‌طور کامل شکاف بین شناسایی و واکنش امنیتی مناسب را تنها با تمرکز بر روی راهبردهای پیشگیری از نقض، تشخیص داده و برطرف نمایند. باید توجه داشت درک این مطلب که نه‌تنها محافظت، بلکه شناسایی و پاسخ به نقض‌ها (نه به‌اندازه اقدامات امنیتی انجام‌شده در ابتدا) بسیار مهم است. سازمان‌ها می‌توانند با برنامه‌ریزی برای موقعیت‌های خطرناک پیش رو، از طریق wargame[۲] (تمرینات تدریجی و نفوذ) و Red Teaming (حملات و نفوذ در دنیای واقعی)، توانایی لازم را برای شناسایی تلاش‌های نفوذ و واکنش‌های مرتبط با نقض امنیتی بهبود ببخشند.

۱/۱. Microsoft Enterprise Cloud Red Teaming

در این مقاله به بررسی نحوه استفاده مایکروسافت از Red Teaming که برای آزمون نفوذ آنلاین سایت در برابر زیرساخت‌های مدیریتی مایکروسافت، سرویس‌ها و برنامه‌های کاربردی می‌باشد؛ می‌پردازیم. همچنین نشان می‌دهیم که چگونه نظارت و اقدامات امنیتی مداوم بر روی Microsoft Azure و Office 365 انجام می‌گیرد. باید به این نکته توجه داشت که هیچ‌یک از اطلاعات کاربری مشتریان توسط Red Teaming و یا آزمون نفوذ به‌طور عمدی مورد هدف قرار نمی‌گیرد. این آزمون‌ها بر روی زیرساخت‌ها، سیستم‌عامل و پلتفرم‌های مورداستفاده مایکروسافت است و برنامه‌ها یا داده‌های میزبانی‌شده توسط Microsoft Azure و Office 365 مورد هدف قرار نخواهند گرفت.

[۲] یک چالش امنیت سایبری و ورزش ذهنی است که رقبا باید از یک آسیب‌پذیری در سیستم و یا برنامه بهره برداری کرده و یا در برابر آن دفاع کنند و یا به سیستم کامپیوتری دسترسی گرفته و یا از دسترسی به آن جلوگیری کنند.

۱/۲ . فراتر از پیشگیری

استراتژی‌ها و تکنولوژی‌های پیشگیری امنیتی نمی‌تواند امنیت را در برابر حملات تضمین کند. این احتمال وجود دارد که یک سازمان مورد حمله قرارگرفته ولی هنوز شناسایی نشده باشد. با استفاده از این فرضیات استراتژی‌ها تشخیص داده شده و پاسخ تغییر می‌یابد، به‌طوری‌که محدودیت‌های زیرساخت‌ها، افراد، فرایندها و تکنولوژی‌های هر سازمان را تحت فشار قرار می‌دهد.

بر اساس گزارش بررسی نقض داده توسط Verizon در سال ۲۰۱۴ ، در ۸۰% موارد سازمان‌هایی که مورد حمله قرارگرفته‌اند، خطرها را شناسایی نکرده‌اند. در عوض آن‌ها توسط یک منبع خارجی مانند مشتری‌ها و یا خدمات امنیتی شرکت‌های ثالث از این موضوع آگاه شده‌اند. در انتها باید ذکر کرد که این آمار مربوط به مواردی است که شناسایی‌شده‌اند و حملات و نفوذهایی که تاکنون ردیابی نشده‌اند را شامل نمی‌شود.

در ادامه این بخش در مورد استراتژی‌های امنیتی جدیدی که در تمام سرویس‌های ابر مایکروسافت مانند Microsoft Azure و Office 365 استفاده می‌شوند، بحث خواهد شد. این استراتژی امنیتی که شکاف فرضی[۳] نامیده می‌شود، روش شناسایی و تغییر پیش‌فرض‌های طراحی، مهندسی و عملیات می‌باشد؛ با فرض اینکه مهاجمان در حال حاضر از آسیب‌پذیری‌ها بهره‌برداری می‌کنند، دسترسی‌ها را افزایش می‌دهند و به‌طور فعال سرویس‌های تولید شده را نظارت می‌کنند.

۲ . روشگان سنتی امنیت

روش‌های سنتی امنیت بیشتر بر پیشگیری تمرکز کرده‌اند. پیشگیری یک استراتژی دفاعی است که هدف آن از بین بردن آسیب‌پذیری‌ها و درنتیجه کاهش نقض امنیتی قبل از وقوع آن است. در خدمات آنلاین مایکروسافت (مانند Microsoft Azure، Office 365، CRM آنلاین و ...) این مورد شامل بهبود مستمر در فرایندهای امنیتی با برنامه‌های چرخهٔ توسعه امنیت[۴] و ضمانت امنیت عملیاتی[۵] است.

مدل‌سازی تهدیدات، تجزیه‌وتحلیل کدهای استاتیک و آزمون امنیت جهت شناسایی، کاهش و مدیریت سطح حملات بسیار مفید هستند، اما آن‌ها تمام خطرات امنیتی را از بین نمی‌برند.

[3] Assume Breach
[4] Security Development Lifecycle
[5] Operational Security Assurance

یکی از مثال‌های استراتژی پیشگیرانه این است که مایکروسافت چگونه محدودیت‌های دسترسی سرپرست/اپراتور را به کارکنانی که نیاز به دسترسی دارند، اعمال نموده است. مثال‌های دیگر شامل مجزا کردن محیط ایمیل کارمندان از محیط تولید و استفاده از ایستگاه‌های کاری تخصصی بسیار امن برای عملیات حساس سازمانی است.

تا جایی که امکان دارد در شرایط مختلف، به‌جای مداخله مستقیم انسانی، فرایندهای مبتنی بر ابزارهای خودکار و حساب‌شده جایگزین می‌گردند. بعضی از نمونه‌های معمول این عملکردها شامل استقرار، اشکال‌زدایی، جمع‌آوری داده‌های عیب‌شناسی و مدیریت سرویس است.

از منظر فناوری‌های عملیاتی، سرمایه‌گذاری‌های پیشگیرانه برای نواقص، احتمال در معرض خطا قرا گرفتن و بهره‌برداری از آن‌ها را کاهش می‌دهد، اما به‌طور کامل نمی‌تواند باعث از بین رفتن آن‌ها گردد. بنابراین درحالی‌که اتخاذ و ادامه بلوغ برنامه‌های مایکروسافت و فناوری‌ها همچنان یک ابزار مهم برای جلوگیری از نقایص امنیتی است، ولی افراد باید قبول کنند که نقض‌های امنیتی بر سازمان، سرویس‌ها و کاربران تأثیر می‌گذارد.

۱/۲ . تهدیدات جدید و در حال ظهور

در طی پنج سال گذشته یک نوع خاص از تهدیدات بسیار مورد بحث قرارگرفته است. تهدید مداوم پیشرفته (APT) یک اصطلاح بود که به‌منظور تلاش برای حمایت از پایگاه‌های نظامی، دفاع از صنعت و شبکه‌های دولتی باهدف تهیه اطلاعات حساس اشاره می‌کرد. اما امروزه APT به‌طور گسترده‌ای برای هر حمله‌ای که به‌طور خاص تنها یک سازمان را مورد هدف قرار داده است، اطلاق می‌گردد. ویژگی مشترک APT عبارت‌اند از:

- برنامه‌ریزی پیشرفته
- هدف خاص و دنباله‌دار
- شناسایی مؤثر
- استفاده از ابزارهای عملی
- مهندسی اجتماعی

امروزه مهاجمان منابع قابل‌توجهی را در اختیار دارند. صرف نظر از پیشرفته بودن مهاجمان، روند حوادث امنیتی از اواخر سال ۲۰۰۹ تاکنون نشان می‌دهد که احتمال وقوع یک حادثه و خطرات ناشی از آن در حال افزایش است. افزایش پیچیدگی و اهداف مورد حمله همراه با تعداد

روزافزون وقوع آن‌ها نشان می‌دهد که نقض‌های امنیتی دیر یا زود بر همه کاربران و سازمان‌ها تأثیر خواهد گذاشت.

در چشم‌انداز تهدیدات فعلی، تنها استفاده از اقدامات پیشگیرانه برای مقابله و شناسایی مهاجمان کافی نیست. علاوه بر این با ابزارهای امنیتی رایج مانند سیستم‌های ضدویروس و تشخیص و ممانعت از نفوذ، کاهش گسترده حفره‌های امنیتی‌ها دشوار است. کنترل‌های لبه شبکه ممکن است که جلوی ورود مهاجمان تازه‌کار را بگیرد، ولی مهاجمان بااستعداد و باانگیزه همیشه ابزارهایی را برای عبور از این کنترل‌ها و ورود به آن را خواهند یافت. درنتیجه معمولاً سازمان‌ها برای مواجهه و پاسخ‌گویی به این نواقص عمیق و گسترده، درمانده می‌شوند.

با تکامل فناوری اطلاعات و رواج ابرها، دیگر نمی‌توان مرزهای سازمان را از طریق محیط شبکه و به‌طور فیزیکی و توسط فایروال‌ها تعریف کرد. اطلاعات سازمان مانند داده‌های حساس و برنامه‌های کاربردی، می‌توانند در هرجایی یافت شوند: در محل سازمان، مراکز داده‌ای خصوصی، در ابرها، در اشتراک با شرکت‌های همکار و انواع دستگاه‌های کاربران. همه این‌ها نیاز به یک استراتژی امنیتی اساساً متفاوت و همچنین یک تغییر در استراتژی‌های مورد استفاده در سازمان‌ها خواهد داشت.

پاسخ‌های صادرشده به نقض‌ها همیشه چالش‌های بسیاری را شامل می‌شوند، ازجمله شناسایی دامنهٔ نقض، اطلاع‌رسانی به‌موقع به ذینفعان و مشتریان، شناسایی داده‌های ازدست داده شده و بازیابی داده‌های حساس و مهم. با ترکیب مهاجمان جدید و تکامل فناوری اطلاعات، واکنش به نقض‌ها، هیچ‌گاه به‌اندازه امروز چالش‌برانگیز نبوده است. بنابراین به‌جای تمرکز سنتی برای جلوگیری از رخنهٔ امنیتی، یک استراتژی مؤثر فرض می‌کند که مهاجم هرگونه مکانیزم دفاعی را نقض نموده است.

۳. روشگان شکاف فرضی[۶]

چشم‌انداز تهدید فعلی مستلزم استراتژی‌هایی است که یک توازنی را برای سرمایه‌گذاری بر روی روش‌های پیشگیرانه و شناسایی و پاسخ ایجاد نماید. از طریق تجزیه و تحلیل دقیق روند امنیتی، مایکروسافت شروع به حمایت و برجسته نمودن نیاز به سرمایه‌گذاری‌های اضافه بر روی فرایندهای امنیتی واکنشی و تکنولوژی‌های تشخیص و پاسخ به تهدیدات در حال ظهور و نه صرفاً جلوگیری از

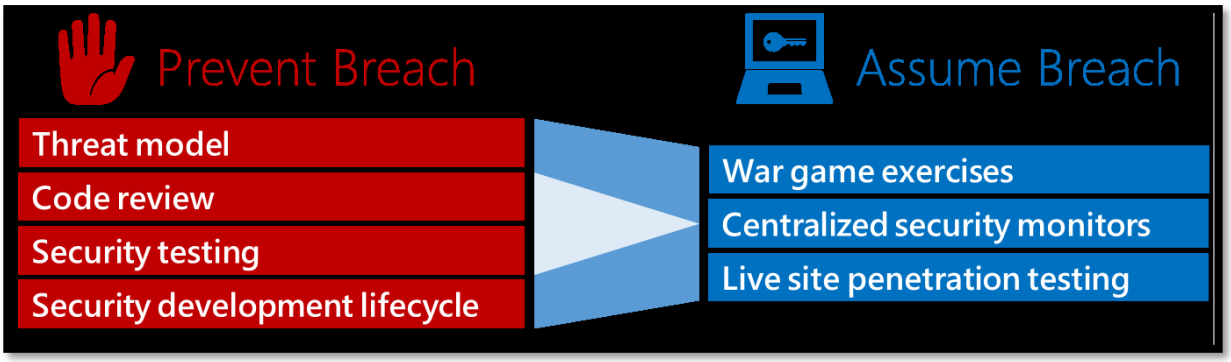
[6] Assume Breach

تهدیدات، نموده است. علاوه بر این در نتیجهٔ تغییر چشم‌انداز تهدیدات و تحلیل‌های عمیق بر روی آن‌ها، مایکروسافت تصمیم به اصلاح استراتژی امنیتی خود نموده است. یعنی علاوه بر جلوگیری از نقض‌های امنیتی، یک استراتژی برای مقابله با نقض در زمانی که در حال رخ دادن است، می‌باشد. درواقع این استراتژی نه به‌عنوان "اگر" در زمان وقوع رویدادهای امنیتی، بلکه به‌عنوان "وقتی" اقدام خواهد نمود.

درحالی‌که مایکروسافت برای مدت‌ها است که از روش شکاف فرضی استفاده می‌کند، اما بیشتر مشتریان از اقداماتی که در پشت‌صحنه برای امن‌تر نمودن ابر مایکروسافت صورت می‌گیرد بی‌اطلاع هستند. شکاف فرضی یک ذهنیتی است که سرمایه‌گذاری‌های امنیتی، تصمیمات طراحی و اقدامات امنیتی عملی را هدایت می‌کند. شکاف فرضی میزان اعتماد به برنامه‌های کاربردی، سرویس‌ها و شبکه‌ها را به‌دلیل در معرض خطر (داخلی و خارجی) بودن، محدود می‌کند. اگرچه استراتژی شکاف فرضی از هیچ‌یک از حفره‌های سرویس مایکروسافت و یا سرویس‌های ابری به‌وجود نیامده است، اما مشخص‌شده است که بسیاری از سازمان‌هایی که در صنعت حضور دارند، با تلاش برای جلوگیری از آن نقض شده‌اند.

درحالی که جلوگیری از شکاف نقش مهمی در عملیات‌های هر سازمان است، این شیوه‌ها باید به‌طور مداوم آزمون شده و تقویت گردند تا به‌طور مؤثر به تهدیدات مانند APTها پاسخ مناسب دهند. برای اینکه سازمان‌ها خود را به‌طور مناسب برای نقض‌ها آماده کنند، باید روش‌های پاسخ امنیتی قوی، قابل تکرار و کاملاً آزمون شده را ایجاد و نگهداری کنند.

با وجود اینکه فرایند امنیتی جلوگیری از حفره‌ها مانند مدل‌سازی تهدید، بررسی کد و آزمون‌های امنیتی در چرخه عمر توسعه امن رایج هستند، اما شکاف فرضی مزایای متعددی مانند انجام و اندازه‌گیری قابلیت واکنش، که به امنیت کلی آن کمک می‌کند، را فراهم خواهد نمود. مایکروسافت قصد دارد تا این کار را از طریق تمرینات wargame و آزمون نفوذ برنامه‌های امنیتی، قابلیت تشخیص و پاسخ را بهبود بخشد.



شکل ۱ : مدل‌های ممانعت از نقض و شکاف فرضی

به‌وسیله شکاف فرضی تمرکز امنیتی به شناسایی و رفع شکاف در موارد زیر تغییر می‌کند:

- تشخیص حمله و نفوذ
- پاسخ به حمله و نفوذ
- بازیابی از نشت اطلاعات، دستکاری داده و به خطر افتادن داده
- پیشگیری از حملات آینده و نفوذ

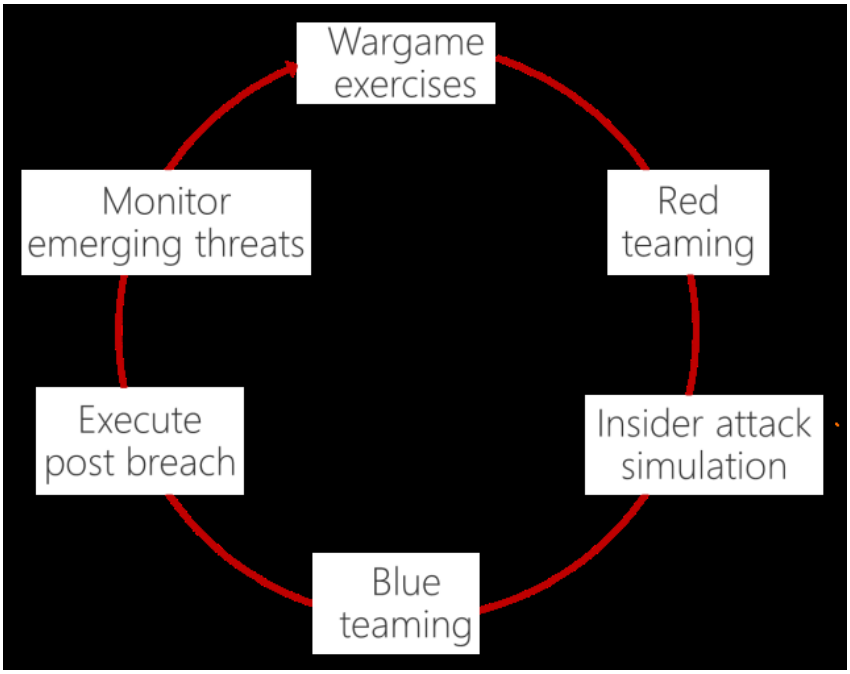
شکاف فرضی تأیید می‌کند که مکانیزم‌های حفاظت، تشخیص و پاسخ به‌درستی اجرا می‌شوند و همچنین می‌تواند باعث کاهش تهدیدات بالقوه با آگاهی از مهاجمان (با استفاده از دارایی‌های قانونی مانند حساب‌ها و دستگاه‌های آسیب‌دیده) گردد.

ماهیت ابرها و مدل‌های محاسباتی ترکیبی اهمیت بیشتری را به قوانین آزمون نفوذ در محیط‌های عملیاتی امن، ازجمله آمادگی برای مقابله با نقض‌ها، وارد می‌کند. از آنجا که بسیاری از جنبه‌های ابر مایکروسافت تحت کنترل مشتریان نیست، مایکروسافت به‌طور مستقیم نه‌تنها بر روی محافظت، بلکه شناسایی و پاسخ به حملات علیه زیرساخت، پلتفرم‌ها و سرویس‌ها کار می‌کند. بنابراین مایکروسافت تمرینات wargame را انجام داده و Red Teaming نیز به‌طور منظم برای ارزیابی و بهبود آمادگی در برابر نقض‌های احتمالی مایکروسافت عمل می‌کند. با شبیه‌سازی حملات دنیای واقعی و همچنین آزمون نفوذ، مایکروسافت قادر است توانایی خود را در مدیریت و رسیدگی به حملات، شناسایی شکاف، تشخیص و پاسخ به آن‌ها را مورد آزمون قرار دهد. مایکروسافت با تمرین کردن پاسخ وقایع امنیتی، نظارت مستمر، جرم‌شناسی و بازیابی، تلاش می‌کند تا توانایی‌های حیاتی موردنیاز خود برای مقابله با نقض‌ها را توسعه دهد.

۳/۱. اجرای شکاف فرضی

شکاف فرضی در سرویس‌های مایکروسافت ابتدا از طریق wargame و سپس تمرینات نقض واقعی که نقض‌های تیم قرمز نامیده می‌شدند و هدف آن‌ها شبیه‌سازی حملات دنیای واقعی بود، انجام می‌شد. آزمون‌های تیم قرمز توانایی مایکروسافت را برای پاسخ به حملات هدفمند و مداوم با هدف کاهش متوسط زمان تشخیص[۷] (MTTD) و متوسط زمان بازیابی[۸] (MTTR) می‌سنجد.

Wargame به‌عنوان یک تمرین آتش‌بازی کوچک در مقابل یک آتش واقعی است. تمرینات تیم قرمز نیز به‌عنوان یک شبیه‌ساز نقض‌های واقعی، کسانی که در ارتباط با آن نقض قرار دارند را آماده می‌کند. تمرینات Wargame و تیم قرمز فرصت‌هایی را برای پاسخگویی به حوادث امنیتی فراهم می‌کنند تا پیش از یک رویداد واقعی به کار گرفته شوند. تمرینات بیشتر باعث مجهزتر شدن و آمادگی در برابر حوادث واقعی خواهد بود.



شکل ۲ : چرخهٔ اجرای شکاف فرضی

[7] Mean-Time to Detect
[8] Mean-Time to Recovery

Wargame .۳/۲

قبل از اختصاص منابع به تیم قرمز در مایکروسافت، فرایندها با تمریناتی به نام Wargame شروع می‌شوند. این تمرینات شبیه به مدل تهدید SDL است. هرچند که برای فرایند پاسخ‌های امنیتی و افراد و سرویس‌هایی که در مواجه با حملات قرار می‌گیرند مجهز شده‌اند. هدف Wargaming بهبود فرایند پاسخ‌دهی امنیتی به رویدادها که با بخش‌های مختلف مایکروسافت در ارتباط می‌باشند، از امنیت تا مهندسی و عملیات، است. هرچه که Wargameها در عمق‌های مختلف آغاز گردد، مشخص می‌شود که کدام بخش‌ها و گروه‌ها ازدست‌رفته‌اند و نیاز به مشارکت و کمک خواهند داشت.

هر شخص یا گروهی که احتمالاً مورد نیاز بوده و در نقض واقعی دخیل است، به‌عنوان یکی از متولیان در تمرینات وارد می‌شود. این نمایندگان نه تنها بخش امنیت که افراد مهندسی و عملیات را نیز شامل می‌شود؛ در بر می‌گیرد بلکه نمایندگانی از تمام بخش‌های شرکت مانند مالی، حقوقی، منابع انسانی، بازاریابی و حتی مدیران را نیز شامل می‌شود. مشارکت مجموعه وسیعی از افراد و گروه‌ها باعث ایجاد روابط لازم میان رشته‌ها و واحدهای تجاری می‌شود که ضمانت توسعه طرح‌های واکنشی را فراهم می‌کند. در بسیاری از موارد این تمرینات منجر به آموزش و ارائه آگاهی در مورد خطرات و نیازهای مرتبط با پاسخ به نقض‌ها در شرکت می‌شود.

هدف اصلی از تمرینات Wargame اطمینان کامل از فرایندهای عملیاتی استاندارد[9] (SOP) و بهبود تشخیص و پاسخ است. سه فاز اصلی از این تمرینات شامل موارد زیر است:

- شناسایی سناریو حمله
- مراحل حمله و پاسخ
- مراحل پس از واقعه

شناسایی سناریو حمله با ایجاد یک لیست از حملات احتمالی آغاز می‌شود. این سناریوهای حمله بسیاری از اشکال مختلف حمله را در بر می‌گیرند. برای مثال برخی از این سناریوها در زیر آورده شده است:

- حملات منع خدمت
- گسترش بدافزار
- اجرای کد از راه دور

[9] Standard Operating Procedures

- به‌دست آوردن اطلاعات مشتری
- مهاجمان داخلی
- به خطر افتادن سرویس‌ها

سناریوها معمولاً از بین موارد شناخته‌شده معمول و یا بر اساس بررسی‌های انجام‌شده بر روی حوادث امنیتی گذشته، انتخاب و اولویت‌بندی می‌شود. بعد از انتخاب سناریوی حمله، از هر گروه یک یا چند نفر (معمولاً حداقل یک نفر از گروه امنیت) در نقش مهاجمان شروع به اجرای حملات و توضیح آن می‌کنند. این شروع حمله و پاسخگویی است.

دیگر اعضای شرکت‌کننده در این روش در نقش دفاعی خواهند بود و مشخص می‌کنند که چگونه می‌توان سناریو حمله را شناسایی و به آن پاسخ دهند. علاوه بر پاسخ‌های دفاعی از مراحل شناسایی، بررسی و بهبود شرایط از حملات انجام‌شده، مهاجمان باید حملات دیگری را بر اساس راه‌حل‌های صورت گرفته توسط گروه‌های دفاعی برای انجام مجدد حملات ترتیب دهند و مدافعان را مجبور به فکر کردن راجع بهروش‌های دیگر شناسایی و پاسخ کنند.

برای مثال اگر برای دفاع پیشنهاد داده شود که آدرس IP مهاجمان مسدود شود، مهاجمان می‌توانند با تغییر آدرس IP منبع بسته‌ها و یا ابزارهای موجود برای این کار مانند بات‌نت‌ها با آدرس IPهای مختلف نسبت انجام حملات موردنظر اقدام کنند. این تلاش‌های مداوم در تمرینات باعث افزایش قابل‌توجه SOP شده و نیازهای سرمایه‌گذاری‌های امنیتی را شناسایی کرده و در بخش‌های مختلف مفید خواهند بود. هرچند این روش بسیار مفید است، اما Wargame نیز محدودیت‌هایی را در اندازه‌گیری‌های خود دارد (مخصوصاً حملاتی که از بیرون صورت می‌گیرند). بنابراین مایکروسافت تلاش‌های زیادی برای آمادگی در برابر حملات پیچیده جهت شناسایی و ارزیابی آن‌ها شروع کرده است. به‌غیر از برخورد با حفره‌ها و نقض‌های امنیتی واقعی، می‌توان به مفهوم دیگری که Red Teaming نامیده می‌شود نیز به‌عنوان راه‌حلی دیگر فکر کرد. Red Teaming به استفاده از تکنیک‌های حمله در دنیای واقعی برای حمله و نفوذ اشاره می‌کند. Red Teaming جنبه‌های تئوری Wargame را دریافت کرده و آن‌ها را به‌صورت واقعی انجام می‌دهد.

Red Teaming .۳/۳

استراتژی‌های شکاف فرضی توسط دو گروه اصلی انجام می‌گیرند، گروه تیم قرمز (مهاجمان) و گروه تیم آبی (مدافعان). رویکرد Red Teaming، آزمون سیستم‌های Microsoft Azure و Office 365 و عمل بر اساس تکنیک‌های مشابه، روش‌ها و رویه‌ها (TTP) به‌عنوان مهاجمان واقعی بر روی زیرساخت‌های تولیدی و بدون دانشی نسبت به زیرساخت، پلتفرم‌های مهندسی با گروه‌های عملیاتی خواهد بود. این آزمون‌های امنیتی قابلیت شناسایی و پاسخ به حملات را بررسی مکرده و همچنین به شناسایی آسیب‌پذیری‌های تولید، خطاهای پیکربندی، پیش‌فرض‌های نامعتبر و یا سایر مسائل امنیتی به روش کنترل‌شده کمک می‌کنند. هر نقض شناسایی شده توسط تیم قرمز به دنبال افشای شکاف موجود بین تیم قرمز و تیم آبی بوده و شناسایی و آدرس‌دهی این شکاف‌ها باعث بهبود قابل‌توجه پاسخ به نقض‌ها خواهد بود.

۳/۳/۱. تیم قرمز

تیم قرمز گروهی از کارکنان تمام‌وقت مایکروسافت هستند که به شناسایی حفره‌ها بر روی زیرساخت، پلتفرم‌ها و برنامه‌ها و سرویس‌های کاربردی مایکروسافت تمرکز دارند. آن‌ها مهاجمان اختصاصی (هکرهای قانونمند) هستند که حملات هدفمند و مداومی را بر روی سرویس‌های آنلاین (زیرساخت، سیستم‌عامل و برنامه‌های کاربردی مایکروسافت و نه برنامه‌های کاربردی و داده‌های مشتریان) انجام می‌دهند.

نقشه راه تیم قرمز برای حمله و نفوذ به محیط‌ها با استفاده از مراحل مختلف حملهٔ مهاجمان در شکل ۳ نشان داده شده است.

شکل ۳: مراحل شکاف

بنابراین تحقیق و درک وقایع صنعت و روند چشم‌انداز تهدیدات به‌منظور آگاهی از آخرین فنون حمله و ابزارهای مورداستفاده توسط مهاجمان بخش مهمی از رویکرد تیم قرمز است. سرویس‌های مایکروسافت به‌عنوان یکی از بخش‌هایی که بیشترین حملات بر روی آن صورت می‌گیرد، اطلاعات زیادی را می‌تواند راجع به حملات در حال ظهور تولید نماید. تیم قرمز از

این تحقیقات و دانش‌های به‌دست آمده می‌تواند نه‌تنها برای مدل‌سازی، بلکه برای تکنیک‌های حملات دنیای واقعی استفاده نماید.

تیم قرمز علاوه بر تحقیق و مدل‌سازی حملات مهاجمان شناخته‌شده، با ایجاد تکنیک‌های جدید برای خود، جهت به خطر انداختن سیستم‌های Microsoft Azure و Office 365 از آن‌ها استفاده می‌نماید. گروه تیم قرمز درست مانند مهاجمان واقعی و متعهد، از تکنیک‌های در حال ظهور و روش‌های ترکیبی جهت ارائه برای ایجاد راه‌حل‌های جدید استفاده می‌نمایند.

چون مهاجمان با استعداد و باانگیزه قادر به نقض اقدامات دفاعی هستند، بنابراین وجود گروه تیم قرمز نیز لازم است. کنترل‌های اولیه می‌تواند جلوی ورود مهاجمان تازه‌کار را بگیرد ولی مهاجمان با استعداد می‌توانند از این کنترل‌ها عبور کنند. بعد از ورود، تیم قرمز در صدد افزایش دسترسی‌های خواهد بود که در حملات عمیق‌تر زیرساخت‌ها می‌تواند مورداستفاده قرار گیرد. تیم قرمز هم می‌تواند مانند مهاجمان خطوط حمله خود را داشته باشند و از آن‌ها برای فرار از تشخیص استفاده نمایند.

برای مثال ممکن است تیم قرمز ابزارهای مخرب مانند ربات‌ها، کنترل‌های راه دور و... را برای دسترسی مداوم به منابع و اطلاعات نصب کند. مکانیزم چنین حملاتی به تیم قرمز این اجازه را می‌دهد که نه‌تنها اطلاعات حساس را حذف نماید، بلکه اطلاعات را به خطر بیندازد.

با توجه به ماهیت حساس و بحرانی این کار، کارکنانی که در تیم قرمز کار می‌کنند باید مطابق بالاترین استانداردهای امنیتی فعالیت نمایند. بنابراین قبل از شرکت در سناریوهای حمله باید اعتبارسنجی‌های اضافی، غربالگری‌ها و آموزش‌های لازم صورت گیرد. اگرچه هیچ‌یک از اطلاعات کاربران توسط تیم قرمز هدف قرار نمی‌گیرد، آن‌ها الزامات دسترسی به اطلاعات مشتری را به‌عنوان کارکنان عملیات سرویس‌دهی به سیستم‌های Microsoft Azure و Office 365 برای استقرار، نگهداری و مدیریت صورت می‌دهند. علاوه بر این تیم قرمز تنها بر روی زیرساخت مدیریت مایکروسافت و سیستم‌عامل آن‌ها حملات را انجام می‌دهند. به‌جای حمله به برنامه‌ها و داده‌های مشتریان، تیم قرمز حملات خود را بر روی برنامه‌ها و داده‌های موجود در ابر که مالکیت آن‌ها در اختیار مایکروسافت است صورت می‌گیرد.

با این وجود تیم قرمز با یک دستورالعمل دقیق رفتار می‌نماید. پنج اصل راهنمای اولیه تیم قرمز به‌صورت زیر است:

- به‌طور عمدی هیچ تأثیر یا خرابی بر روی موارد توافق‌نامه سطح خدمات مشتریان (SLA) صورت نمی‌گیرد.
- بطور عمدی هیچ تغییر یا دسترسی به داده‌های مشتریان صورت نمی‌گیرد.
- اقدامات خرابکارانه به‌طور عمدی صورت نمی‌گیرد.
- حفاظت‌های امنیتی محلی تضعیف نمی‌گردند.
- اطلاعات مربوط به آسیب‌پذیری‌ها و اطلاعات حساس تنها باید بین اعضای تیم قرمز به اشتراک گذاشته شود.

علاوه بر این تیم قرمزِ سیستم‌های Microsoft Azure و Office 365، باید مجموعه‌ای از قوانین مربوط به تعهد[10] را که به‌منظور اطمینان از اجرای کدهای بالا است، دنبال نمایند. این قوانین را مدیران رده‌بالای مایکروسافت در اختیار گذاشته‌اند.

برخی از معیارهای امنیتی حساس که تیم قرمز باید برای پیگیری نقض‌ها در نظر داشته باشد، به‌صورت زیر است:

- متوسط زمان به خطر افتادن[11] (MTTC)
- متوسط زمان ارتقاء دسترسی[12] (MTTP)

متوسط زمان به خطر افتادن، زمان بین شروع یک تمرین تا تلاش موفقیت‌آمیز برای در اختیار گرفتن آن منبع توسط تیم قرمز را اندازه‌گیری می‌کند. متوسط زمان ارتقاء دسترسی زمان بین شروع تمرینات تا زمانی است که منبع موردنظر کاملاً درخطر بیافتد. به‌عنوان‌مثال در محیط‌های مبتنی بر Active Directory این برابر زمانی است که تیم قرمز دسترسی مدیر دامنه را به دست می‌آورد و یا Domain Controller را به خطر می‌اندازد.

می‌توان MTTP را به‌عنوان "Game Over" در بازی‌ها در نظر گرفت، زیرا اکثر سازمان‌ها خود را برای مواجهه با این سطح از نقض آماده نکرده‌اند. بااین‌حال باید توجه کرد که سناریوهای "Game Over" تنها سناریوی قابل استفاده توسط تیم قرمز نیست. اهداف تیم قرمز می‌تواند شامل سرقت اطلاعات، حملات منع سرویس و یا به خطر انداختن مشتریان در سطوح مختلف

[10] Rules of Engagement
[11] Mean Time to Compromise
[12] Mean Time to Privilege Escalation

باشد. علاوه براین می‌توان MTTP و MTTC را به ازای هر تمرین و یا به ازای هر قربانی محاسبه نمود.

نقش تیم قرمز مایکروسافت شناسایی حفره‌های کنترل‌های امنیتی اهداف است. محاسبه MTTC و MTTP به مایکروسافت این اجازه را می‌دهد تا روند بهبود مداوم سیستم‌ها را پیگیری نماید.

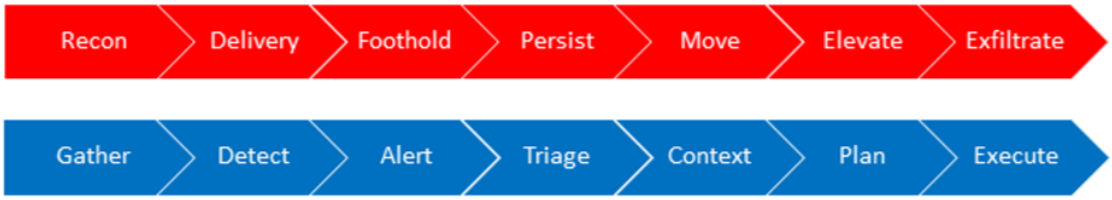
تیم قرمز با استفاده از برجسته‌کردن نظارت‌های امنیتی و شکاف‌های بازیابی نقاط ضعف امنیتی، ابزارهای پاسخ به رویدادها و فرایندها را بهبود می‌بخشد. درنتیجه تیم قرمز با شناسایی ریسک‌های تجاری و منابع دفاعی موردنیاز، اولویت‌ها و نیازهای سرمایه‌گذاری را مشخص می‌کند.

۳/۳/۲. تیم آبی

تیم آبی شامل یک مجموعه اختصاصی از پاسخ‌دهندگان امنیتی یا اعضای گروه واکنش، مهندسی و عملیاتی هستند. صرف‌نظر از تشکیل این گروه، آن‌ها به‌طور مستقل از تیم قرمز عمل می‌کنند. تیم آبی نیز دارای استانداردهای امنیتی تأیید شده است و از آخرین ابزارها و تکنولوژی‌های روز برای شناسایی و پاسخ به حملات و نفوذها استفاده می‌کند. درست مانند حملات دنیای واقعی، اعضای تیم آبی نیز از زمان و نحوه حملات و یا متدها و ابزارهای مورد استفاده تیم قرمز آنگاه نیستند. بنابراین تیم آبی به‌صورت ۲۴ ساعت شبانه‌روز و ۳۶۵ روز سال آماده واکنش نسبت به حملات تیم قرمز ، درست مانند مهاجمان واقعی می‌باشد. زمانی که یک مهاجم مانند تیم قرمز به یک محیط حمله می‌کند، تیم آبی موارد زیر را در اسرع وقت انجام می‌دهد:

- شواهدی که بر اساس رفتار مهاجمان به‌دست آمده را جمع‌آوری می‌کند.
- شواهدی که نشان‌دهنده به خطر افتادن سیستم است را شناسایی می‌کند.
- به گروه‌های مهندسی و عملیاتی هشدارهای لازم داده می‌شود.
- مجموعه‌ای از هشدارها را برای اطلاع از نیاز به بررسی‌های بیشتر اعلان می‌کند.
- جمع‌آوری اطلاعات از محیطی که موردحمله قرارگرفته است.
- با استفاده از یک طرح پالایشی نسبت به خارج کردن مهاجمان اقدام می‌شود.
- اجرای طرح پالایشی و بازیابی حفره‌های امنیتی.

شکل ۴ مراحل موازی برای اقدامات لازم جهت خارج کردن مهاجمان و پاسخ به رویدادهای امنیتی را نشان می‌دهد:



شکل ۴: مراحل پاسخگویی به شکاف

به‌طور خلاصه می‌توان گفت که حفره‌های شناسایی شده توسط تیم قرمز اجازه می‌دهد تا توانایی‌های تیم آبی جهت شناسایی و پاسخ به حملات واقعی مشخص گردد. مهم‌تر از آن، این اجازه را به تیم آبی می‌دهد تا قبل از بهره‌برداری از حفره‌ها و نقض‌ها توسط مهاجمان واقعی، تمرینی برای حوادث واقعی صورت گرفته باشد. علاوه بر این، به‌عنوان یکی از نتایج نقض‌های مشخص شده توسط تیم قرمز ، گروه تیم آبی می‌تواند آگاهی خود را از موقعیت موجود افزایش دهد تا از حملات آینده مهاجمان در امان باشند و پاسخ مناسب را به آن‌ها بدهند.

در طول فرآیند تشخیص و پاسخ، تیم آبی دانش مورد نیاز خود را نسبت به شرایط تولید می‌کند که می‌توان نمودِ آن را در شرایط واقعی و تلاش برای دفاع از حملات واقعی مشاهده کرد. اغلب این کارها از طریق تجزیه و تحلیل داده‌ها و اقدامات جرم شناسانه بعد از شناسایی و پاسخ به حملات تیم قرمز ، توسط تیم آبی انجام می‌شود.

درست مانند چگونگی شناسایی تیم قرمز برای شناسایی شکاف‌های امنیتی، تیم آبی نیز با توجه به توانایی‌هایش نسبت به شناسایی و پاسخ به این شکاف‌های امنیتی اقدام می‌کند. از زمانی که تیم قرمز حملات دنیای واقعی را شروع می‌کند، تیم آبی بر اساس توانایی‌های خود می‌تواند با آن برخورد مناسب کند. مانند تیم قرمز ، معیارهای قابل‌اندازه‌گیری توسط تیم آبی عبارت‌اند از:

- مدت زمان تخمینی برای تشخیص[۱۳] (ETTD)
- مدت زمان تخمینی برای بازیابی[۱۴] (ETTR)

[13] Estimated Time to Detection
[14] Estimated Time to Recovery

دلیل استفاده از "زمان تخمینی" برای نقض‌های کشف شده توسط تیم آبی ، صرف نظر از اینکه آیا حفرهٔ مورد نظر شناسایی شده است، این است که تیم آبی نمی‌تواند دقیقاً مشخص کند که حمله چه زمانی رخ داده است؟ آیا مهاجمان از سیستم مورد نظر خارج شده‌اند؟ و آیا نقض مورد نظر به‌طور کامل رفع شده است؟

این‌ها مواردی هستند که پاسخ‌های امنیتی را به چالش کشیده‌اند. در واقع این مانند پازلی است که نمی‌توان مشخص کرد که تصویر نهایی به چه صورت است و یا تعدادی از قطعات برای کامل کردن آن از دست رفته باشند.

با افزایش آگاهی از چشم‌انداز کلی نسبت به تهدیدات و افزایش دیدگاه نسبت به شرایط محیطی که در آن فعالیت می‌کنند، تیم آبی می‌تواند روش‌های اقدامات امنیتی مربوط به رخدادهای واقعی را تقویت کند و آمادگی خود برای مقابله با آن‌ها را افزایش دهد.

۳/۳/۳. تیم قرمز در مقابل تیم آبی

برخلاف آزمون نفوذ سنتی، تیم قرمز تلاش می‌کند تا حملات دنیای واقعی مانند "Fog of War"[۱۵] را شبیه‌سازی کند. این بدان معناست که تیم آبی نمی‌داند که حملات تیم قرمز چه زمانی اتفاق خواهد افتاد و بالعکس. زمانی که تیم قرمز یک مجموعه دارایی را با حملات خود به خطر می‌اندازد، ممکن است یک سری اخطارهای امنیتی را اعلان کرده باشند که تیم آبی از آن‌ها اطلاع ندارند.

تیم قرمز ممکن است عمداً هشدارهایی را برای تأیید پیش‌فرض‌های نظارتی یا تکنیک‌های انحرافی ایجاد نماید. همچنین ممکن است که تیم قرمز برای مشاهده پاسخ‌های انجام شده به حملات مانند تغییر رمز عبور، به خطر انداختن دارایی‌هایی که قبلاً به خطر افتاده بودند و یا آزمون رفع مسدودیت‌های قبلی این اعلان‌ها را راه‌اندازی نمایند.

در این رابطه نقض‌های تیم قرمز می‌تواند اثرات تشخیص و پاسخ به آن‌ها را آشکار نماید. مقادیر معیارهای متوسط زمان تشخیص و متوسط زمان پاسخگویی تنها بعد از افشای اقدامات صورت گرفته توسط تیم قرمز و تیم آبی می‌تواند محاسبه شوند. تیم قرمز برای رسیدن به تشخیص و پاسخ کامل باید موارد زیر را در نظر داشته باشد:

---

[۱۵] برای توصیف عدم اطمینان درباره آگاهی از موقعیت تجربه شده توسط شرکت کنندگان در ارتباط با توانایی خود، توانایی رقبا و اهداف رقبا استفاده می‌شود.

- طیف وسیعی از TTPهایی که سازمان توسط مهاجمان با آن‌ها مواجه شده است (و یا خواهد شد) را شبیه‌سازی نماید.
- به‌کارگیری TTPهای مختلف در محل‌های مختلف زنجیره امنیتی سازمان که می‌توانند با آن‌ها مواجه شوند.
- به‌کارگیری پیچیدگی‌های فنی و پیچیدگی‌های عملیاتی
- تکرار حملات و تمرینات برای بهبود شرایط تشخیص و پاسخ و اطمینان از ماندگاری آن‌ها برای حملات و مهاجمان واقعی.

به‌منظور اطمینان از این‌که تمرینات در تعامل با تیم آبی انجام می‌شود، تیم قرمز می‌تواند به‌طور عمدی باعث تشخیص و پاسخ‌گویی به حملات شود. این معمولاً زمانی اتفاق می‌افتد که تیم قرمز به اهداف خود از حملات دست‌یافته است ولی هیچ واکنشی را از سمت تیم آبی مشاهده نکرده است.

به‌عنوان نمونه تیم قرمز می‌تواند عمداً یک اسکنر Anti-Malware را برای مثال بر روی Domain Controller برای اعلان اخطار از وجود فایل مخرب در آن، به‌کار بیندازد. اعلان یک اخطار بر روی قسمت مهمی مانند Domain Controller باید قسمت پاسخگویی تیم آبی را فعال نماید. تا زمانی که تیم آبی در حال کار بر روی رویداد امنیتی است، ممکن است هیچ پاسخی صادر نشود.

در حالت ایده‌آل، تیم آبی نمی‌تواند تشخیص دهد که رویداد امنیتی از طرف تیم قرمز است و یا یک مهاجم واقعی. هر زمان که ممکن باشد تیم آبی باید حوادث امنیتی را به‌عنوان یک حمله واقعی قلمداد کند.

شبیه‌سازی حملات دنیای واقعی بهترین روش برای محافظت در دنیای واقعی است.

۳/۳/۴. پس از واقعهٔ نقض امنیتی تیم قرمز

در پایان کار هر نقض امنیتی توسط تیم قرمز ، دو گروه تیم قرمز و تیم آبی برای ارزیابی نقض‌ها و حفره‌های بررسی‌شده، گرد هم می‌آیند. در این مرحله هر دو گروه تکنیک‌ها و آموزش‌های به‌دست آمده را به اشتراک می‌گذارند. تیم قرمز تمام جزئیات در مورد زمان، حفره‌های محیط، دارایی‌هایی که توسط این گروه در اختیار قرار گرفتند و کنترل‌های به‌دست آمده را مشخص می‌کند. علاوه بر این تیم آبی نیز جزئیاتی در مورد نحوه و زمان تشخیص حملات و حفره،

دارایی‌های به خطر افتاده و سازوکارهای پایداری تیم قرمز وهمچنین اقدامات انجام‌شده برای پاسخ به نقض‌های پیش آمده را مشخص می‌کند. در نتیجه این یکی از بخش‌های حساس تیم قرمز است که می‌تواند جزئیات نقض و بازخورد حملات موفقیت‌آمیز (یا غیر موفقیت‌آمیز) را از گروه دفاعی دریافت کند. توانایی هر دو گروه برای مقایسه نکات و یادداشت‌های ثبت شده از تمرینات بسیار حائز اهمیت هستند.

فقط در پایان کار افشای کامل جزئیات رخ می‌دهد. همچنین در این زمان می‌توان معیارهای MTTD و MTTR را محاسبه نمود. برای مثال با مقایسه بین MTTC از تیم قرمز و ETTD از تیم آبی می‌توان زمان دقیق MTTD را به دست آورد. این معیارهای تشخیص و پاسخ که در طول و پس از حادثه محاسبه می‌شوند، برای ارزیابی خطرات تجاری و بهبود شکاف‌ها که بخشی از اهداف تمرینات بوده مفید خواهند بود. بسیاری از بررسی‌ها جهت مشخص کردن نیازهای سرمایه‌گذاری و آسیب‌پذیری‌های موجود، بعد از این زمان و در ارتباط با هر دو گروه صورت می‌گیرد.

با هر رخنه‌ای که توسط تیم قرمز مشخص می‌گردد، هر دو گروه سرمایه‌گذاری‌های امنیتی را برای تشدید حملات آینده، محدود نمودن مهاجمان واقعی و افزایش سرعت تشخیص و پاسخ به حملات، به کار می‌گیرند. به عبارت دیگر افزایش زمان MTTC و کاهش MTTD و MTTR. آخرین اقدام در این مرحله، تهیه گزارش از تمام مراحل توسط دو گروه است. این گزارش‌ها شامل جدول زمانی نقض‌ها، خلاصه تأثیرات کسب‌وکاری این تمرینات، و همچنین فهرست دقیق آسیب‌پذیری، یافته‌ها و سرمایه‌گذاری‌های موردنیاز برای بهبود تشخیص نقض و پاسخ به آن است.

۴. اصول امنیت

یکی از مزایای اصلی Red Teaming تقویت متخصصین امنیت و منابع هک اخلاقی است. مانند سایر حرفه‌ها، کارکنان بخش مهندسی و عملیاتی ممکن است دارای مهارت‌های حمله و نفوذ نباشند. در مایکروسافت مهندسین و کارکنان به‌خوبی با SDL/OSA و همچنین معیارهای مشترک مهندسی[۱۶] آشنا هستند، اما تیم قرمز وظیفه آزمون‌های امنیتی بر روی محصولات محیط خارجی را نیز بر عهده دارد. زیرا در غیر این صورت مقابله با آن‌ها بسیار دشوار خواهد بود.

[16] Common Engineering Criteria

مایکروسافت با سرمایه‌گذاری بر روی Red Teaming با تمرکز بر شناخت، ارتباطات و بهره‌گیری از آخرین تهدیدات در حملات صورت گرفته، تلاش می‌کند به‌طور مداوم آزمون و قابلیت‌های پاسخ‌گویی را با توجه به اصول کلیدی زیر بهبود بخشد:

- مقاومت در برابر استراتژی‌های امنیتی در سناریو حملات ایستا و یا فرض کنید که مهاجمان تنها از طریق موقعیت‌های ثابت وارد می‌شوند.
- به‌کارگیری لایه‌های کنترل امنیتی مکمل که باعث اثر بخشی و بهبود دفاع می‌شود.
- تعداد و توزیع‌های کنترل‌های امنیتی مهم‌تر از کارایی تک‌تک آن‌ها است.
- به‌جای جلوگیری از حمله باید به دنبال علت تأخیر پاسخگویی بود.

۵. خلاصه

شرکت‌های صنعتی در سراسر جهان با واقعیت تلخی مواجه شده‌اند که ممکن است در شرایط ثابت و در معرض خطر فعالیت کنند. این واقعیت که برخی از شرکت‌ها هنوز هم متوجه نشده‌اند که در معرض خطر و حمله قرار دارند، حتی وضعیت را بدتر نیز می‌کند. چشم‌انداز تهدیدات امروز نیاز به کاهش حملات، ازجمله تهدیدات داخلی دارد. برای کاهش متوسط زمان تشخیص و بازیابی نقض در سازمان‌ها نیاز به تغییرات ضروری است.

این مقاله نشان داد که سازمان‌ها نیاز دارند تا به‌سرعت شکاف‌های امنیتی را شناسایی نمایند. مایکروسافت از طریق استراتژی امنیتی شکاف فرضی، به‌صورت مداوم به‌دنبال سرمایه‌گذاری گسترده و عمیق در امنیت است. همه سازمان‌ها می‌توانند از راهکارهای مشابه برای مقابله با تهدیدات و حملات در حال ظهور استفاده کنند.

مایکروسافت توانایی‌های خود برای مدیریت حوادث امنیتی را با برنامه‌ریزی‌های پیشرفته در برابر خطرات احتمالی و شبیه‌سازی حمله و نفوذ با Wargame و تیم قرمز فعال توسعه می‌دهد. تیم قرمز با کشف حفره‌های امنیتی و بهره‌برداری از آن‌ها و همچنین ارائه شواهد مشخص، سناریوهای حملات واقعی را شبیه‌سازی می‌کند.

چالش تیم آبی، توانایی تشخیص و پاسخ به این حملات است. با انجام تمرینات این دو گروه در ارتباط با یکدیگر، سازمان‌های امنیتی می‌توانند بر روی روش‌های حملات تمرکز کنند و سازوکارهای پاسخ به حملات مهاجمان را کامل‌تر نمایند.

در حال حاضر Red Teaming یکی از بخش‌های اساسی مایکروسافت برای زیرساخت‌ها، پلتفرم‌ها و سرویس‌ها است. تیم قرمزمربوط به Microsoft Azure و Office 365، از مهاجمان متمایز هستند و به مایکروسافت اجازه می‌دهند تا امنیت را بهبود بخشند، دفاع در برابر حملات را تقویت نمایند و کارایی برنامه‌های ابر را افزایش دهند.

از طریق حملات فعال منظم و آزمون‌های نفوذِ لحظه‌ای، حفره‌های شناسایی‌شده توسط تیم قرمز، ابزاری برای تمرین پاسخگویی به رویدادهای امنیتی و آمادگی در برابر آن‌ها و همچنین اندازه‌گیری تأثیرات آن‌ها در حملات دنیای واقعی است. مشتریان می‌توانند اطمینان داشته باشند که مایکروسافت به‌طور مداوم نسبت به بهبود حفاظت، تشخیص و پاسخ به حملات، برای ارائه سرویس‌های امن‌تر ابری تلاش می‌کند.

۶. پیوست

۶/۱. تفاوت تیم قرمز و آزمون نفوذ

در تکنیک‌های استاندارد آزمون نفوذ معمولاً از ابزارهای رایج برای بهره‌برداری از آسیب‌پذیری‌ها استفاده می‌شود، اما به‌ندرت توانایی‌های یک مهاجم مورد توجه قرار می‌گیرد. آزمون نفوذ معمولاً تنها در یک بازه زمانی است و پس از آن هیچ دغدغه‌ای برای حملات و پاسخی که به آن‌ها داده می‌شود، در محیط وجود دارد. فعالیت‌های تیم قرمز همیشه ادامه دارد و با اتمام یک حمله، کار به پایان نمی‌رسد. Red Teaming معمولاً مواردی را شامل می‌شود که در روش‌های آزمون نفوذ نادیده گرفته می‌شود. (خلاصه این موارد در زیر آمده است)

جدول ۱ :مقایسه تیم قرمز و آزمون نفوذ

	تیم قرمز	آزمون نفوذ
ماندگاری	ایجاد مکانیزم پایدار برای حفظ دسترسی و ارزیابی کامل حفره‌ها.	زمانی که حملات با موفقیت صورت گرفت، فعالیت‌ها اتمام می‌یابد.
ابزارها	به‌طور مداوم از آسیب‌پذیری‌های کشف شده و ابزارهای جدید استفاده می‌کنند.	تنها از ابزارهای موجود در آن زمان استفاده می‌کند و سپس تا چرخه بعدی آزمون باید صبر کرد.
فعالیت‌های پس از حمله	از حملات برای خرابکاری و سوءاستفاده از اطلاعات مهم و به‌کارگیری آن‌ها برای حملات دیگر استفاده می‌شود.	به‌عنوان هکرهای کلاه سفید هستند. تنها تلاش می‌کنند تا وارد شوند و پس از آن کاری نمی‌کنند.
اجتناب از تشخیص	آزمون‌های پویا برای جلوگیری از شناسایی شدن صورت می‌گیرند.	آزمون‌های ایستا ممکن است برای جلوگیری از شناسایی شدن صورت نگیرند و در صورت معلوم شدن متوقف شوند.
دانش شناخته شده	به دنبال آسیب‌پذیری‌های شناخته نشده و مواردی که مورد استفاده قرار نگرفته است، می‌باشد. از دانش داخلی و فردی افراد و ابزارهای سفارشی شده برای سیستم‌های ناشناخته استفاده می‌کند.	مایل است تا سیستم‌های امنیتی شناخته شده را مورد آزمون قرار دهد. برای پی بردن به اینکه آیا موارد امنیتی به‌درستی اعمال شده‌اند؟ و یا آسیب‌پذیری‌های شناخته شده بر روی سیستم وجود دارد؟
دامنهٔ آزمون	بر روی تمام لایه‌ها و تمام سیستم‌های پشت صحنه، حملات انجام می‌گیرد.	تقریباً هیچ‌گاه به‌طور کامل به سیستم‌های تولیدی حمله صورت نمی‌گیرد. اغلب بر روی سیستم‌هایی با پیکربندی مشابه آزمایشی تست می‌شود.
انگیزش	هیچ پیش فرضی از محیط ندارد. تلاش می‌کند تا همه قسمت‌ها را در معرض خطر قرار دهد.	فرضیاتی راجع به محیط ایجاد می‌نماید. ممکن است جاهایی که عنوان نشده است، مورد آزمون قرار نگیرد.
نتایج	معیارهای MTTD، MTTP، MTTC و MTTR محاسبه می‌شود. شواهد دقیق در مورد زمان و چگونگی نقض محیط، دارایی‌هایی که به خطر افتاده است و اینکه آیا تشخیص و پاسخ موفق آمیز بوده است، ارائه می‌گردد.	تنها موارد مورد آزمون و نتیجه آن‌ها (شکست/موفقیت) را ارائه می‌دهد.