معرفی خدمت مسابقات کشف نقص امنیتی

نسخه ۱٫۰

آذر ۹۹


بسم الله الرحمن الرحیم

فهرست مطالب

مقدمه

در راستای استفاده بهینه از ظرفیت متخصصین امنیت فضای تولید و تبادل اطلاعات برای کشف آسیب پذیری و ارتقاء سطح امنیت سازمان‌ها، خدمت «مسابقات کشف نقص امنیتی» به عنوان یکی از خدمات امنیت فضای تولید و تبادل اطلاعات تعریف می‌گردد. این خدمت در قالب طرح ساماندهی خدمات امنیت فضای تولید و تبادل اطلاعات، به عنوان یکی از گرایش‌های خدمات عملیاتی امنیت فضای تولید و تبادل اطلاعات است. در این سند به بیان شرایط متقاضی و اجرای این خدمت که به صورت برگزاری مسابقه کشف نقص و آسیب پذیری بر روی سامانه‌ها است، پرداخته می‌شود.

ایجاد و مدیریت فضای مسابقه‌گونه به منظور کشف نقص و آسیب‌پذیری بر روی سامانه‌هایی که اقدامات تست نفوذ و امن‌سازی بر روی آنها انجام پذیرفته باشد، باعث افزایش اثربخشی کشف نقاط آسیب پذیر و رفع آن می‌گردد.

در خدمت «مسابقات کشف نقص امنیتی»، مشتری سامانه‌ها و سرویس‌های خود را در قالب نام دامنه و آدرس IP به شرکت دارای پروانه فعالیت در این گرایش اعلام می‌کند و شرکت با برگزاری مسابقه در محدوده آزمون نفوذ مشخص شده توسط مشتری، نقص‌های کشف شده توسط شرکت کنندگان در مسابقه را ارزیابی و در صورت صحت به اطلاع مشتری می‌رساند تا اقدامات لازم برای رفع آن‌ها صورت پذیرد. همچنین بر اساس سطح نقص گزارش شده، جوایزی از طرف مشتری به کشف کننده نقص مذکور تعلق می‌گیرد.

فرآیند درخواست، ارزیابی، صدور و نگهداری پروانه فعالیت در این گرایش از خدمات امنیت فضای تولید و تبادل اطلاعات، مطابق با آیین نامه ساماندهی خدمات امنیت فضای تولید و تبادل اطلاعات است. لازم به ذکر است که یک شرکت نمی تواند هر دو پروانه فعالیت «آزمون و ارزیابی امنیتی» و «مسابقات کشف نقص امنیتی» را همزمان داشته باشد و نیز فعالیت اقتصادی مشترک در حوزه ارائه این خدمات با دیگر شرکت‌های دارای پروانه فعالیت داشته باشد.

۱. اصطلاحات

۱-۱ **خدمت باگ بانتی**: خدمتی که در آن سامانه/سامانه‌های یک نهاد/سازمان/شرکت توسط مشارکت کنندگان تست نفوذ می‌شود. مدیریت این خدمت توسط چارچوبی که پلتفرم باگ بانتی نامیده می‌شود و در اختیار شرکت متقاضی پروانه می‌باشد، انجام می پذیرد. باگ بانتی به سه صورت زیر قابل انجام است:

- باگ بانتی عمومی[1]: که در آن مشتری سامانه‌ای را برای تست نفوذ معین می‌کند که دسترسی به آن از طریق اینترنت برای عموم آزاد می‌باشد.
- باگ بانتی خصوصی[2]: که در آن مشتری سامانه‌ای را برای تست نفوذ معین می‌کند که دسترسی به آن برای عموم آزاد نبوده و نیاز به مجوز خاصی دارد (به عنوان نمونه سامانه بر روی شبکه محلی قرار دارد و یا از طریق VPN قابل دسترس است). همچنین در شرایط خاص ممکن است مشتری درخواست کند که برای سامانه‌ای که در دسترس عموم قرار دارد، تست نفوذ از مسیر مشخصی تحت مالکیت شرکت برگزار کننده مسابقه انجام پذیرد.
- باگ بانتی محدود[3]: مسابقه‌ای است که با وجود در دسترس عموم بودن سامانه، به درخواست مشتری، بدون اعلام عمومی و با دعوت از شماری از متخصصین منتخب، برگزار می‌گردد.

۱-۲ **متقاضی دریافت پروانه**: شرکتی است که ارائه خدمت باگ بانتی را بر عهده می‌گیرد. شرکت می‌بایست دارای چارچوبی باشد که کلیه فعالیت‌های برگزاری مسابقه از قبیل ثبت نام اعضا، پرداخت بانتی و دریافت گزارش از طریق آن انجام شود. همچنین وظیفه اعتبار سنجی آزمون‌های انجام شده توسط اعضاء، بر عهده شرکت می‌باشد.

۱-۳ **مشارکت کنندگان:** که به اختصار در این سند اعضاء نامیده می شود شامل افرادی است که در چارچوب باگ بانتی شرکت متقاضی پروانه، ثبت نام کرده‌اند و در مسابقات کشف نقص امنیتی شرکت می کنند.

۱-۴ **دستگاه‌های زیرساختی:** کلیه نهادها و سازمانهای مشمول ماده «۲۲۲» و بند «الف» ماده «۲۳۱» قانون برنامه پنجم توسعه جمهوری اسلامی ایران

۲. شرایط و تعهدات متقاضی پروانه فعالیت

۲-۱ متقاضی دریافت پروانه فعالیت باید بر روی چارچوب (پلتفرم) باگ بانتی خود، توسط شرکتی که دارای پروانه فعالیت آزمون ارزیابی باشد، آزمون نفوذپذیری انجام دهد. همچنین مسابقه دائمی کشف نقص بر روی سامانه خود برگزار کند.

---

[1] - Public

[2] - Private

[3] - Limited

۲-۲ دارنده‌ی پروانه‌ی فعالیت موظف است تمامی مدارک و نتایج ارائه خدمت را با رعایت اصول امنیتی جمع‌آوری، مدیریت و به صورت امن ذخیره‌سازی کند و متعهد به عدم افشای آنها باشد.

۲-۳ دارنده‌ی پروانه‌ی فعالیت، مسئول حفظ اطلاعات بهره برداران مسابقات و مشارکت کنندگان در فرآیند کشف نقص و آسیب پذیری است و حق انتشار اطلاعات را به هیچ نهادی غیر از نهادهای ذی‌صلاح ندارد.

۲-۴ مسئولیت جلوگیری از دسترسی غیرمجاز به اطلاعات مربوط به آسیب‌پذیری‌ها و نقاط ضعف سامانه‌ها که در پلتفرم نگهداری می‌شوند، برعهده دارنده پروانه فعالیت است.

۲-۵ دارنده پروانه فعالیت موظف به رعایت بی طرفی و عدم ذینفع بودن در سازمان مشتری و نیز در کشف نقص و آسیب‌پذیری در سامانه‌ها می‌باشد.

۲-۶ دارنده پروانه فعالیت موظف است تا افرادی که بعنوان اعضاء در سامانه ثبت نام می‌کنند را با استفاده از سازوکار مطمئن احراز هویت کند.

۲-۷ دارنده پروانه فعالیت، مجاز به شرکت دادن افراد موجود در فهرست نفرات غیر مجاز اعلامی توسط مراجع ذی صلاح در مسابقات نمی باشد.

۲-۸ داوران مسابقات، باید حتما عضو شرکت متقاضی دریافت پروانه فعالیت خدمت «مسابقات کشف نقص امنیتی» بوده و دارای مهارت‌ها و قابلیت‌های زیر باشند:

- تخصص در حوزه تست نفوذ وب
- تخصص در حوزه تست نفوذ موبایل
- تخصص در حوزه تست نفوذ شبکه
- تخصص در حوزه مقاوم‌سازی و امن‌سازی
- تخصص در تحلیل و مدیریت ریسک
- تخصص فارنزیک

۳. الزامات اجرای خدمت

دارنده پروانه فعالیت ارائه خدمت «مسابقات کشف نقص امنیتی» موظف است که برای کلیه مشتریانی که جزء مشمولین ماده «۲۲۲» و بند«الف» ماده «۲۳۱» قانون برنامه پنجم توسعه جمهوری اسلامی ایران هستند، الزامات زیر را رعایت کند:

۳-۱ دارنده‌ی پروانه‌ی فعالیت برای ارائه خدمت به دستگاه‌های زیرساختی، تنها مجاز به ارائه خدمت به دستگاه‌های زیرساختی است که تاییدیه مرکز افتا را برای انجام مسابقه بر روی سامانه مورد نظر دریافت کرده باشند.

۳-۲ دارنده‌ی پروانه‌ی فعالیت موظف است تا ساختار و تیم مجری مسابقه پروژه خود را به صورت دقیق و با ذکر مسئولیت هر فرد پیش از انعقاد قرارداد به مشتری اعلام کند. تیم مجری مسابقه حق شرکت در مسابقه را ندارند.

۳-۳ موارد ذیل را در قرارداد با مشتری می‌بایست تعیین و مشخص کند:

- نوع مسابقه شامل عمومی، خصوصی و یا محدود می‌باشد. برای دستگاه‌های زیرساختی، مسابقه عمومی، مجاز نمی‌باشد.
- سامانه‌های تحت مسابقه شامل سامانه‌های عملیاتی یا سامانه‌های شبیه سازی شده (با اولویت سامانه‌های شبیه‌سازی شده)
- وجود یا عدم وجود اطلاعات حساس در سامانه تحت آزمون
- نحوه نظارت و مانیتورینگ سیستم‌های تحت آزمون
- اولویت‌بندی باگ‌ها براساس آخرین نسخه سیستم امتیازدهی آسیب‌پذیری مشترک (CVSS) به حداقل چهار سطح حیاتی، بالا، متوسط، کم
- هزینه (پاداش) برای هر باگ براساس سطح‌بندی صورت گرفته شده
- مدت زمان انتظار برای پرداخت هزینه برای هر باگ بعد از دریافت گزارش آن
- تست مجدد به منظور اطمینان از باگ‌های رفع شده (در صورت تمایل مشتری)

۳-۴ برای مسابقاتی که مشتری آن از دستگاه‌های زیرساختی باشد، قبل از شروع مسابقه، قرارداد می‌بایست توسط شرکت برگزار کننده مسابقه به تائید مرکز مدیریت راهبردی افتا برسد.

۳-۵ برای مسابقاتی که مشتری آن از دستگاه‌های زیرساختی است، حداکثر زمان تایید و اعلام گزارش از زمان کشف نقص می‌بایست به شرح زیر باشد:

- باگ حیاتی: ۲ روز کاری
- باگ با اهمیت بالا: ۳ روز کاری
- باگ با اهمیت متوسط: ۴ روز کاری
- باگ با اهمیت کم: یک هفته کاری

۳-۶ دارنده پروانه فعالیت موظف است به صورت هفتگی، یک نسخه از گزارشات ارسالی نقص‌های کشف شده در سامانه‌های متعلق به دستگاه‌های زیرساختی را به مرکز مدیریت راهبردی افتا و

گزارشات مربوط به دستگاه‌های غیرزیرساختی دولتی را به سازمان فناوری اطلاعات ایران ارسال نماید.

۳-۷ قبل از ارائه خدمت، کلیه راهنمایی‌ها و هشدارهای لازم درخصوص ذخیره سازی لاگ رخدادهای امنیتی شناسایی شده، بهمراه تشریح پیامدهای احتمالی ناشی از عدم مدیریت لاگ، لازم است توسط دارنده پروانه فعالیت به صورت مکتوب به مشتری اعلام گردد. بدیهی است عواقب ناشی از نداشتن مدیریت لاگ، بر عهده مشتری خواهدبود.

۳-۸ قبل از برگزاری مسابقه باید این اطمینان حاصل شود که از سامانه‌های تحت مسابقه نسخه پشتیبان تهیه شده و روال بازیابی آنها در نظر گرفته شود. لازم است تا مسئولیت اجرای این امر در قرارداد به صورت دقیق بیان شده باشد.

۳-۹ قبل از برگزاری مسابقه باید مکانیزمی در سمت مشتری پیاده‌سازی شود که با استفاده از آن بتوان تغییرات ایجاد شده در پایگاه‌های داده، فایل‌های آپلود شده برروی سامانه‌ها و تغییرات در فایل‌های حیاتی سامانه‌های مورد آزمون را تشخیص داد. لازم است تا مسئولیت اجرای این امر در قرارداد به صورت دقیق مشخص گردد.

۳-۱۰ در صورتیکه مسابقه به صورت خصوصی صورت گیرد موارد ذیل می‌بایست در رابطه با سامانه-ها/سرویس‌های تحت مسابقه مشتری رعایت گردد:

- دسترسی اعضاء به سامانه‌های مشتری می‌بایست از طریق پلتفرم و یا شبکه تحت کنترل و نظارت شرکت دارای پروانه فعالیت انجام گیرد.
- هویت شرکت کنندگان در مسابقه برای شرکت دارای پروانه فعالیت، احراز شده باشد.
- قبل از دسترسی به سامانه‌های مشتری، اعضاء می‌بایست توسط پلتفرم، احراز هویت گردند.
- کلیه فعالیت‌های کاربر بعد از احراز هویت، می‌بایست قابل ردیابی باشد.
- در شرایطی که ارتباط با سامانه‌های تحت مسابقه رمزنگاری شده باشد، لاگ ارتباطات با جزئیات دقیق به صورت متن آشکار می‌بایست در سمت مشتری ذخیره گردد. (خود مشتری می‌تواند این مورد را در شبکه خود انجام دهد و یا از شرکت دارای پروانه بخواهد آن را در مسیر ارتباطی انجام دهد)

۳-۱۱ در صورتیکه مسابقه بصورت محدود صورت پذیرد، موارد زیر می‌بایست در رابطه با سامانه-ها/سرویس‌های تحت مسابقه مشتری رعایت گردد:

- دارنده پروانه فعالیت لازم است از اعلام عمومی جزئیات برگزاری مسابقه و نتایج آن خودداری نماید.

- برگزاری مسابقه با دعوت از گروهی از متخصصین عضو پلتفرم، توسط دارنده پروانه فعالیت صورت پذیرد.
- لازم است پلتفرم برگزاری مسابقات، امکان دسته بندی متخصصین و برگزاری مسابقات محدود، با حضور گروه های مختلف متخصصین را داشته باشد.
- شرکت کنندگان در مسابقه متعهد باشند تا جزئیات برگزاری مسابقه و نقص‌های امنیتی را در رسانه‌ها و شبکه‌های اجتماعی منتشر ننمایند.

۱۲-۳ دارنده پروانه فعالیت لازم است بر اساس دامنه پروژه نسبت به ارزیابی و مشخص کردن ریسک‌های موجود اقدام کند.

۱۳-۳ دارنده‌ی پروانه‌ی فعالیت موظف است قبل از انتشار اطلاعاتی در مورد نقص‌ها و آسیب‌پذیری‌های کشف شده (در رابطه با سامانه‌های مشتری) در پلتفرم خود، تاییدیه مربوطه را از مشتری دریافت کند.

۱۴-۳ دارنده‌ی پروانه‌ی فعالیت موظف است بعد از ارائه خدمت با توجه به نتایج، نسبت به ارائه توصیه‌های امن‌سازی (شامل چگونگی رفع آسیب‌پذیری‌ها) و پاک‌سازی دامنه آزمون به متقاضی خدمت اقدام کند. همچنین در صورت تمایل مشتری، نسب به رفع آسیب‌پذیری‌ها اقدام کند.

۱۵-۳ دارنده پروانه فعالیت موظف است مسئولیت رعایت ملاحظات فارنزیک در سامانه‌های خود را داشته و در صورت وقوع رخداد شواهد را در اختیار مرکز مدیریت راهبردی افتا و یا نهادهای مرتبط قضایی قرار دهد.