ارزیابی برنامه های کاربردی برای مقابله با خطرات امنیتی

برنامه ریزی

سازمان ها باید اطمینان حاصل نمایند که برنامه های کاربردی از امنیت لازم برخوردار می باشند. رویه های ارزیابی برنامه های کاربردی باید شامل تست برنامه کاربردی باشد که نتیجه آن پذیرش برنامه یا رد آن می باشد. برنامه ارزیابی مخاطرات که به تصمیم گیری در خصوص تاثیر امنیتی برنامه های کاربردی تلفن همراه کمک می کند باید بر روی منابع، داده ها، شبکه و دستگاه های پردازشی سازمان ها انجام شود.

گام اول:

تعیین مجموعه ای از الزامات امنیتی منحصر به فرد برای سازمان با در نظر گرفتن معیارهای زیر:

- شرایطی که تحت آن برنامه کاربردی می تواند استفاده شود یا شرایطی که تحت آن برنامه کاربردی نباید به کار برده شود.
- داده هایی که در دسترس برنامه کاربردی قرار دارد چگونه امن خواهد بود.
- توابع زیرساخت بیسیم چگونه است و چگونه امن می باشد.
- آیا دارایی های حیاتی بر روی دستگاه های تلفن همراه قرار دارند یا نه.
- سطح قابل قبول ریسک برای برنامه ها.
- تصمیم گیری در خصوص الزامات امنیتی که مورد نیاز برنامه ها است. این مساله به سازمان ها اجازه می دهد تا پس از انجام تست متوجه شوند که الزامات برآورده شده است یا نه.
- آیا آسیب پذیری هایی در برنامه کاربردی وجود دارد که بتوان با در نظر گرفتن کنترل های امنیتی دیگر احتمال سوء استفاده از آن را کاهش داد. (این کنترل های امنیتی می تواند بخشی از معماری دستگاه های سیار سازمان یا کنترل های امنیتی خود دستگاه تلفن همراه باشد.)
- ارزیابی راه حل موجود در سیستم مدیریت دستگاه تلفن همراه برای تایید این نکته که کدام الزام امنیتی توسط این راه حل پوشش داده می شود.
- تعیین الزامات امنیتی و جریم خصوصی خاص برای سازمان
- تعیین مجوزهای کاربران برای استفاده از برنامه کاربردی
- در حال حاضر چه سطحی از تست امنیت برنامه مورد قبول است.
- چه نوع حملاتی باعث نگرانی سازمان می شود (اطلاعات و عملیاتی در نظر گرفته شود که در صورت به خطر افتادن آن ها، بر روی کارمندان و افراد مرتبط با آن سازمان و کسب و کار سازمان تاثیر خواهد گذاشت)

گام دوم:

در این مرحله باید محدودیت های فرآیند سنجش برنامه کاربردی مشخص شود. رویه به کار برده شده برای ارزیابی برنامه های کاربردی بدون شک تاثیر مثبتی بر روی وضع امنیتی سازمان دارد با این وجود هیچ رویه ای وجود ندارد که بتواند تمامی ضعف های بالقوه را ارزیابی کرده و امنیت کامل را تضمین نماید.

- باید دانست که فرآیند ارزیابی با توجه به پیامدهای امنیتی چه مواردی را تامین می کند و چه مواردی را تامین نمی کند.
- ارزیابی هایی که به صورت دستی توسط افراد انجام می شوند نباید کمتر از میزان واقعی تخمین زده شود. این امر بخش مهمی از فرآیند است.
- تنها به ارزیابی های خودکار بسنده نشود، به کارگیری افراد برای دیدن رفتارهای جامع و کلی برنامه ها مورد نیاز است.

- کیفیت ارزیابی متناسب با به کار بردن ترکیبی از ابزارهای تست خودکار و تجارب امنیتی افراد متخصص است.
- از به کار بردن تنها یک ابزار و یک فرآیند تست اجتناب شود زیرا استفاده از فرآیندها و ابزارهای مختلف بهترین نتیجه را می دهد.
- باید به کارمندان درباره محدودیت های فرآیند تست برنامه کاربردی آموزش داده شود.

گام سوم:

در این مرحله باید تیمی از متخصصین تشکیل داده تا بتوانند مسئولیت اجرای این فرآیند را برعهده بگیرند و هم چنین باید بودجه موجود برای فرآیند تست برنامه را در نظر گرفت.

- استخدام افراد مناسب با تخصص های مورد نیاز (تخصص های امنیت تلفن همراه، امنیت نرم افزار و اطلاعات مورد نیاز است)
- هزینه ها باید به طور کامل ارزیابی شده و بودجه مورد نیاز تخصیص داده شود.