شرکت های تولید کننده نرم افزار امروزه در حال تولید میزان انبوهی از نرم افزار ها هستند و هر یک سعی می کنند به مرور زمان سیستم های خود را از لحاظ کارایی ، دقت ، سرعت و عملکرد صحیح بهبود بخشند .

اما متاسفانه تولیدکنندگان نرم افزار به مهمترین بخش حیات یک نرم افزار که امنیت آن است توجه چندانی ندارند ،گاه به یک کلمه عبور اکتفا می کنند و گاه هزینه های بسیار بسیار ناچیزی از پروژه خود را به شرکت های امنیتی اختصاص می دهند تا آنها با توجه به بوجه مورد نظر کاری برایشان بکنند در حالیکه هر محصول نرم افزاری در نهایت می بایست در بسته ای امن جای گرفته و راهی بازار مصرف شود و نمی تواند با اطمینان بی مورد و اما ، اگر محصول عریان از حصار های امنیتی را وارد بازار مصرف نمود و انتظار داشت که مشتریان برای آن هزینه نمایند .

اینجا، جایی است که امنیت نرم افزار مطرح می شود. امنیت نرم افزار یک نظام جوان است که خصوصیات امنیتی نرم افزار را هنگامی که در حال طراحی، آزمایش، پیاده سازی و بکارگیری است، مورد خطاب قرار می دهد.

یعنی در دوره زمانی تولید نرم افزار یا Software Development Life Cycle (SDLC). این امر شامل فعالیت های امنیتی زیادی در مراحل مختلف در SDLC، مانند مدل کردن تهدید، مدیریت خطر و آزمایش های امنیتی است.

در اینجا چند پیشنهاد برای بهبود امنیت نرم افزارها، آورده شده است

۱- تولید کنندگان نیاز دارند که تیم امنیت IT خود را تا جایی که امکان دارد از اولین مراحل طراحی، درگیر کنند. هنگامی که شما سعی خود را می کنید تا در مورد ساخت چیزی تصمیم بگیرید، اندیشیدن در مورد نحوه سوءاستفاده یا تخریب آن آسان نیست. شما مجبورید مانند یک شخص امنیتی فکر کنید. خوب، اعضای تیم امنیت IT شما، فعالیت حرفه ای خود را برروی مطالعه نحوه تخریب چیزها سپری کرده اند، و می توانند به شما کمک کنند تا بفهمید نرم افزار شما با چه نوع حملاتی ممکن است مواجه شود.

۲- مشابها، به اعضای تیم امنیت اجازه دهید در طراحی تست های امنیتی به شما کمک کنند. و در اینجا (فقط) منظور یک تست نفوذ یک هفته قبل از بکارگرفتن نرم افزار نیست! منظور انجام تمام تست های بسیار جدی است که شما در مورد نرم افزارها انجام می دهید.

۳- به تاکتیک هایی که تیم عملیات می تواند برای افزایش امنیت نرم افزار شما بکارگیرد، توجه کنید. برای مثال، آیا فایل ها، کتابخانه های اشتراکی (مثلا فایلهای DLL. در ویندوز) یا اجزاء دیگری که کاملا برای امنیت نرم افزار شما مهم هستند، وجود دارند؟ تیم عملیات لزوما نخواهد دانست که آنها چه هستند مگر اینکه شما به ایشان بگویید. این تیم با دانستن اینکه قسمت های باارزش و حیاتی نرم افزار شما کجا قرار دارند، می توانند کنترل دسترسی به فایل، ثبت وقایع (شامل تشخیص نفوذ) را تضمین کنند و همچنین هنگامی که قسمتی دچار انحراف می شود به افراد ذیصلاح اطلاع داده می شود.

پس می توان گفت امنیت هر محصول نرم افزاری تضمین کننده طول عمر شرکت تولید کننده آن نرم افزار است .

واژه امنیت نرم افزار شامل دو قسمت عمده است .

۱- تعیین سطح دسترسی به کمک کلمه عبور امضا و اثر انگشت و....

۲- ایجاد محدودیت انتشار (کپی)

حسینی

شرکت مهندسی یاقوت سبز ایرانیان

http://www.balascd.com