بررسی ابعاد مختلف رویکرد «کشف رویدادها» و اطمینان از سلامت اطلاعات

بخش سوم مقاله امنیت در دنیای وب

بررسی ابعاد مختلف رویکرد «کشف رویدادها» و اطمینان از سلامت اطلاعات

در دو بخش قبلی از مجموعه امنیت در دنیای وب در رابطه با تعاریف امنیت صحبت کردیم و رویکرد پیشگیری را به صورت کامل بیان کردیم. در این بخش، رویکرد کشف رویدادها را با تفصیل بیشتری توضیح می‌دهیم و با عناصر تشکیل‌دهنده آن بیشتر آشنا می‌شویم. پس از شناخت این عناصر، معیارهای مشترک را به عنوان نمونه‌ای از استاندارد این شیوه معرفی و آن را از دید نرم‌افزارهای وبی، بررسی خواهیم کرد.

کشف رویدادها و اطمینان از سلامت اطلاعات

این شیوه نگرش را می‌توان به این صورت بیان کرد: همواره باید دانست چه اتفاقاتی پیش از این افتاده و چه اتفاقاتی در حال رخ دادن است؟ آیا رویدادی اتفاق افتاده است که باعث غیرقابل اطمینان شدن اطلاعات شده باشد یا خیر؟ اصل و پایه این رویکرد به

این صورت است که سعی می‌کند با دانستن اینکه چه اتفاقی در چه زمانی، توسط چه کسی در چه موقعیت و وضعیتی روی داده یا در حال روی دادن است، این قابلیت را در اختیار ذینفعان نرم‌افزار قرار دهد که بتوانند وضعیت امنیتی نرم‌افزار را بررسی کنند و نتیجه‌گیری کنند آیا اطلاعات تحت تاثیر، هنوز قابل اطمینان است یا خیر؟

این رویکرد، اعتماد به نرم‌افزار را بر مبنای شفافیت نسبت به رویدادها قرار داده است و سعی می‌کند با دخیل کردن مفاهیم هر کسب‌وکار بر روی ساختارهای نرم‌افزاری، اعتماد به نرم‌افزار را برای کاربر اضافه کند. این رویکرد، نرم‌افزار را به 2 بخش تقسیم می‌کند: رویدادهایی که روی اطلاعات اتفاق می‌افتد. در واقع اگر بخواهیم تعریفی از نرم‌افزارهایی داشته باشیم که سیستم‌های اطلاعاتی را مکانیزه می‌کنند این تعریف می‌تواند کاملا درست باشد. این رویکرد می‌خواهد همواره ارتباط منطقی تعریف شده در سیستم‌های اطلاعاتی بین کاربران، اطلاعات و رویدادها در طول حیات یک اطلاعات، موجود و قابل پیگرد باشد.

بر اساس این نگاه این رویکرد به دنبال اهداف زیر است:

1. **رصد کردن وضعیت امنیتی و رویدادهایی که در نرم‌افزار در حال وقوع است.**
2. **اعتماد به خدشه‌دار نشدن اطلاعاتی که نرم‌افزار در حال مدیریت آن است.**
3. **همیشه در دسترس بودن تاریخچه حیات زندگی یک اطلاعات.**
4. **انکار ناپذیری برای رویدادهایی که بر روی اطلاعات رخ داده است.**

در واقع در این رویکرد، صحبتی از حمله و پیشگیری از آن وجود ندارد. چیزی که مهم است حفاظت از یکپارچگی اطلاعات در اختیار نرم‌افزار است. این رویکرد، کاربران را

در قالب نقش‌هایی در نظر می‌گیرد که در طول زندگی نرم‌افزار باعث وقوع رویدادهایی بر روی اطلاعات می‌شوند. آنها اطلاعات را ایجاد و آنها را ویرایش می‌کنند، اطلاعات را مشاهده و در نهایت در مواقعی آنها را حذف می‌کنند. این رویدادها پایه‌ای‌ترین رویدادهایی است که هر سیستم اطلاعاتی درگیر آن است و هر رویداد دیگری باعث این چهار رخداد اصلی در نرم‌افزارها می‌شود.

رویکرد کشف رویدادها، به دنبال افزودن مجموعه‌ای از قابلیت‌ها به نرم‌افزار است که بر اساس این بتوان هدف‌های بالا را تحقق بخشید و در واقع بتوان شیوه‌ای را تهیه کرد که خود اطلاعات، قابل اعتماد باشند.

برای این رویکرد قابلیت‌ها به 3 دسته تقسیم می‌شوند:

- قابلیت‌هایی که تاریخچه رویدادها را در بر می‌گیرند.
- قابلیت‌هایی که یکپارچگی داده‌ها را تعریف و در صورت مخدوش شدن، آنها را شناسایی می‌کنند.
- قابلیت‌هایی که نقش‌ها و دسترسی‌های اطلاعاتی و عملیاتی نقش‌ها را شفاف و بر اساس آن، انکارناپذیری را محقق می‌کنند.

با مجموعه این قابلیت‌ها شفاف‌سازی مورد نیاز امنیت به وجود می‌آید و هم نرم‌افزار و هم کاربران می‌توانند تفکیکی بین اطلاعات قابل اعتماد و غیر قابل اعتماد داشته باشند.

قابلیت‌های دسته اول به طور کامل بر روی مفهوم ممیزی رویدادها استوارست؛ به این معنی که هر رویدادی که روی یک موجودیت اطلاعاتی اتفاق می‌افتد را بتوان پیگیری

کرد. تفاوتی بین لاگ‌کردن رویداد و ممیزی کردن آن وجود دارد. ممیزی ساختار اطلاعاتی کامل‌تری نسبت به لاگ رویداد دارد و می‌تواند اطلاعات بسیار بیشتری از رویدادهای اتفاق افتاده را ارائه کند.

در رابطه با اطلاعات ممیزی نیاز است که مشخص باشد بر روی کدوم شی، بر اساس چه رویدادی، توسط چه کسی، در چه زمانی، چه بخش‌هایی از اطلاعات شی تغییر کرده است و این اطلاعات قبل و بعد از رویداد چه مقادیری داشته و در حال حاضر چه مقداری دارند. در واقع اطلاعات ممیزی نه تنها مشخص‌کننده رویداد اتفاق افتاده است؛ بلکه اطلاعاتی از تغییرات مربوط به موجودیت در حال تغییر نیز نگه می‌دارد. به این ترتیب می‌توان شفافیتی در رابطه با تاریخچه تمامی رویدادها همراه با اینکه چگونه بر موجودیت اطلاعات موثر بوده‌اند، بدست آورد.

قابلیت‌های دسته دوم به این منظور تعریف می‌شود که بتوان مخدوش شدن اطلاعات را از مسیرهایی غیر از مسیر نرم‌افزار تشخیص داد. تمامی‌تغییرات نرم‌افزار ممیزی تولید می‌کنند؛ اما اگر کسی از مسیری غیر از مسیر نرم‌افزار، اطلاعات را تغییر دهد باید بتوان آن را کشف کرد تا اطلاعات نامطمئن کشف شوند. این قابلیت‌ها مجموعه‌ای از ساختارها، الگوریتم‌ها و مفاهیمی‌است که بر اساس آن می‌توان مخدوش شدن اطلاعات را تشخیص داد.

قابلیت‌های دسته سوم به منظور ایجاد انکارناپذیری برای رویدادها در نظر گرفته شده‌اند. در این قابلیت‌ها تعاریفی از دسترسی‌ها بیرون می‌آید که به نقش‌ها داده می‌شود و نقش‌ها به کاربران داده می‌شوند. بر اساس این قابلیت‌ها می‌توان کشف کرد که آیا

کاربر خاصی توانسته اطلاعاتی را مشاهده کند یا عملیات خاصی را انجام دهد یا خیر ؟ امضای اطلاعات یا رویدادها شیوه‌ای از تضمین انکارناپذیری تغییرات اعمال شده بر روی اطلاعات است.

پیش از این در ایران این رویکرد برای نرم‌افزارهای در حال توسعه، رویکرد قالب بود. علت آن هم استفاده از نرم‌افزارهایی بر روی بستر سیستم عامل بود؛ اما به مرور زمان با توجه به اینکه نرم‌افزارها آرام آرام از بستر سیستم عامل به بستر وب نقل مکان کردند اهمیت رویکرد پیشگیری بالا رفت و رویکرد کشف به عنوان رویکرد درجه 2 شناخته شد.

این مورد اهمیت دارد که بدانیم که مخصوصا در دنیای وب اهمیت پیشگیری بسیار بیشتر از اهمیت کشف رویدادهای غیرمجاز یا مخدوش شدن اطلاعات است. در واقع رویکرد کشف باید رویکردی برای تکمیل مفهوم امنیت در بستر وب باشد. این مورد در رابطه با نرم‌افزارهای سایر پلتفرم‌ها برعکس است و اتفاقا رویکرد قالب باید رویکرد کشف باشد. به عنوان مثال برای تولید سیستم عامل یا پایگاه داده، این رویکرد بسیار حائز اهمیت است؛ اما برای بستر وب آن چیزی که بسیار اهمیت دارد رویکرد پیشگیری است. امنیت در این بستر بر اساس پیشگیری است و کشف تکمیل نیازمندیهای سیستم اطلاعاتی را برای اجرای درست امنیت در کسب‌وکار تعریف می‌کند.

معیار مشترک

معیار مشترک (Common Criteria) چارچوبی است برای امنیت کامپیوتری که با

شناسه ISO/IEC 15408 به استانداردی بین‌المللی تبدیل شده است. این چارچوب، یک هدف ارزیابی را با توجه به مجموعه‌ای از اسناد به هم مرتبط بر اساس یک یا چند پروفایل حفاظتی را برای مشخص‌کردن سطح اطمینان آنها در یک چارچوب تعریف شده ارزیابی می‌کند.

بر اساس آنچه که گفته شد نیاز است که مفاهیم بیان شده تعریف شوند:

1- هدف ارزیابی: یک محصول یا سیستم است که موضوع ارزیابی است.

2-پروفایل حفاظتی: سندی است که در آن مجموعه نیازمندی‌های امنیتی در کلاس‌هایی که در استاندارد آورده شده است تعریف می‌کند. در واقع استاندارد معیار مشترک امنیت را کلاس‌بندی کرده است و بر اساس پروفایل‌های حفاظتی مختلف، مشخص می‌شود که برای چه نوع هدف‌هایی، چه نیازمندی‌هایی برای هر کلاس باید وجود داشته باشد.

3-نیازمندی‌های تضمین امنیت: شرح اقدامات انجام شده در طول توسعه و ارزیابی محصول برای اطمینان از عملکردهای امنیتی هدف ارزیابی است. در واقع چارچوبی از اسناد هستند که به صورت منطقی بین آنها ارتباط وجود دارد. این اسناد معرفی‌کننده تمامی‌جوانب مربوط به هدف ارزیابی هستند.

در هر هدف برای شروع فرایند ارزیابی ابتدا باید این اسناد را ارزیابی و بر اساس آنها درک درستی در رابطه با هدف ارزیابی پیدا کرد. مهمترین این اسناد به شرح زیر است:

1. **سند هدف امنیتی:** سندی است که در آن مجموعه کلی معماری و الزامات امنیتی

که هدف ارزیابی ادعای وجود آنها را در خود دارد، آورده می‌شود. این سند ادعا می‌کند که چه الزاماتی از چه پروفایل‌های حفاظتی را در خود جای داده است.

2. **سند پیکربندی:** مشخص‌کننده ساختار نسخه‌بندی و پیکربندی قطعات مختلف هدف ارزیابی است.
3. **سند راهنما:** راهنمای استفاده از هدف ارزیابی است.
4. **سند واسطها:** این سند، ارتباط بین سند راهنما و سند هدف امنیتی را برقرار می‌کند و در آن مشخص می‌شود که هر قابلیتی که در راهنما آورده شده کدامیک از الزامات امنیتی مربوط به سند هدف امنیتی را پیاده‌سازی کرده است.
5. **سند آزمون:** سندی است که نتایج آزمون ارزیابی امنیتی در آن آورده شده و درآن انطباق و عدم انطباق هدف ارزیابی با ادعاهای امنیتی اعلام شده در سند هدف امنیتی آورده شده است.

1- نیازمندی‌های عملکردهای امنیتی: مشخص‌کننده توابع امنیتی است که به عنوان الزامات در سند پروفایل حفاظتی آورده می‌شود. هر کدام از این توابع در یک کلاس استاندارد تعریف می‌شوند و مشخص‌کننده شیوه پیاده‌سازی الزام موجود در استاندارد در پروفایل حفاظتی است.

2-سطوح اطمینان ارزیابی: رتبه‌بندی عددی در رابطه با توصیف عمق و سختی ارزیابی ارائه می‌دهد. این چارچوب چند سطح اطمینان تعریف می‌کند و برای هر سطح اطمینان قوانین و فرآیندهایی را به منظور میزان اطمینان در نظر می‌گیرد و بر این اساس، هدف ارزیابی را در یکی از این سطوح اطمینان قرار می‌دهد.

این استاندارد به گونه‌ای طراحی شده که هر سیستم یا محصول کامپیوتری را بتوان بر اساس آن ارزیابی کرد. روال این استاندارد به این شکل است که برای هر نوع محصول یا سیستم یک پروفایل حفاظتی از الزامات امنیتی سیستم یا محصول ارائه می‌شود و تولیدکنندگان بر اساس این الزامات امنیتی، مجموعه‌ای قابلیت به سیستم یا محصول خود اضافه می‌کنند. سپس یک سطح تعریف شده امنیتی را انتخاب و براساس آن از آزمایشگاه درخواست آزمایش می‌کنند. برای این کار، محصول را همراه با مستندات مورد نیاز در اختیار آزمایشگاه قرار می‌دهند و در سند هدف امنیتی وجود الزامات امنیتی را براساس پروفایل حفاظتی ادعا می‌کنند. آزمایشگاه ادعاهای امنیتی تولیدکننده را بررسی می‌کند و در صورت تطبیق ادعاها سند آزمون را تولید و در آن مشخص می‌کند که آیا محصول یا سیستم، الزامات را رعایت کرده است یا خیر.

همانطور که تا الان متوجه شده‌اید این استاندارد برای هرگونه محصول یا سیستم تولیدی در کامپیوتر است؛ اما علت اینکه ما این استاندارد را در این مقاله آوردیم این است که در ایران دولت، این استاندارد را برای تمامی محصولات کامپیوتری در نظر گرفته است و نرم‌افزارهای تحت وب را نیز از طریق این استاندارد، ارزیابی امنیتی می‌کند.
تولیدکنندگان نرم‌افزارهای وبی نیز برای دریافت گواهی امنیت باید بر روی این استاندارد، فعالیت کنند. از این رو، آشنا بودن خوانندگان با این استاندارد و شیوه نگاه آن برای دانستن دنیای این استاندارد کمک‌کننده خواهد بود.

باید توجه داشت این چارچوب اعلام می‌کند که تضمینی برای امنیت ارائه نمی‌دهد. علت آن هم ساده است ، ایجاد یک چارچوب برای تمامی‌محصولات و سیستم‌ها این چارچوب را به سطحی از انتزاع رسانده است که عملا نمی‌تواند تمامی ابعاد پلتفرم‌های

مختلف را در بر بگیرد و در عمل بسیاری از رویکردهایی که در مرحله پیشگیری وجود دارد در آن جایگاهی ندارند.

این چارچوب سطوح اطمینان زیر را تعریف کرده است:

- سطح یک – قابلیت‌های محصول یا سیستم تست می‌شود.
- سطح دو – ساختارهای طراحی محصول یا سیستم تست می‌شود.
- سطح سه – وجود مهندسی امنیت در طراحی سیستم یا محصول با شیوه‌های مشخصی مورد تست قرار می‌گیرد که هدف آن، افزایش اطمینان امنیتی در طراحی است.
- سطح چهار- سیستم یا محصول بر اساس روش‌های مشخصی طراحی، تست و بازرسی می‌شود.
- سطح پنج- سیستم یا محصول بر اساس روش‌های نیمه رسمی‌طراحی و تست می‌شود.
- سطح شش- سیستم یا محصول بر اساس روش‌های نیمه رسمی طراحی، تست و بازرسی می‌شود.
- سطح هفت- سیستم یا محصول بر اساس روش‌های رسمی طراحی، تست و بازرسی می‌شود.

در این سطوح همانطور که مشخص شده، سعی در این است که شیوه‌های تولید محصول کامپیوتری، امن شوند. این استاندارد سعی می‌کند که مهندسی امنیت را به مرور و در طی سال‌ها در تولیدکنندگان به عنوان روش‌های رسمی تولید محصول قرار

دهد و به این ترتیب، میزان اطمینان به محصول یا سیستم را بالا برد. برای اینکه بیشتر بتوان این سطوح‌بندی را درک کرد به صورت ساده در سطح یک محصول به صورت جعبه سیاه مورد تست قرار می‌گیرد و فقط درست کارکردن الزامات امنیتی مورد تست است.

در سطح دو علاوه بر درست کارکردن، الزامات درست طراحی شدن آنها هم تست می‌شود؛ بنابراین نیاز است اطلاعات طراحی محصول در آزمایشگاه بررسی شود. در سطح سوم علاوه بر دو، سطح اولِ تست جعبه سفید نیز صورت می‌گیرد؛ به عنوان مثال اگر یک نرم‌افزار در حال آزمون باشد تمامی‌کدهای آن نیز مورد تست قرار می‌گیرد تا اطمینان حاصل شود که پیاده‌سازی طراحی‌های سطح دو نیز به درستی انجام گرفته است. به همین ترتیب این چارچوب آرام آرام تمامی‌بخش‌های خط تولید محصولات کامپیوتری را به ابزار امنیت تجهیز می‌کند و حضور امنیت را در تمامی‌این بخش‌ها تست می‌شود. در سطح هفتم، کل خط تولید با استفاده از روش‌های رسمی امن در برگرفته می‌شوند.

سطح چهارم این چارچوب، آخرین سطحی است که رسیدن به آن توجیه اقتصادی دارد. محصولاتی که هم باید تجاری باشند و هم در ذات خود به امنیت نیاز دارند در این سطح قرار می‌گیرند. سیستم عامل‌ها و یا پایگاه داده‌ها از این جنس محصولات هستند. به عنوان مثال مایکروسافت برای نسخه‌های ویندوز خود سعی می‌کند در این سطح، گواهینامه دریافت کند به این دلیل که این سطح برخلاف سایر سطوح، توجیه اقتصادی دارد. به صورت میانگین، رسیدن از سطح یک به دو بین 5 تا 10 ماه زمان و بین 80 تا 100 هزار دلار هزینه نیاز دارد و رسیدن از سطح سه به سطح چهار نیاز به 9 تا 24 ماه

زمان و بین 150 تا 350 هزار دلار هزینه دارد. این هزینه و زمان بسیار زیاد است به همین دلیل سطح پنج به بعد بسیار غیر اقتصادی است.

پروفایل‌های حفاظتی برای انواع محصولات و سیستم‌ها از دستگاه‌های امنیتی بستر شبکه و توکن‌های نگهدارنده کلید خصوصی تا انواع نرم‌افزارهایی مانند سیستم عامل‌ها و پایگاه داده‌ها تولید می‌شوند. محصولات و سیستم‌ها به منظور اعمال آن‌ها در نرم‌افزارها شروع به استفاده از این پروفایل‌های حفاظتی می‌کنند.

ارائه پروفایل حفاظتی برنامه‌های کاربردی تحت شبکه توسط معاونت امنیت فضای تولید و تبادل اطلاعات نهاد ریاست جمهوری

برای نرم‌افزارهای بستر وب در ایران، معاونت امنیت فضای تولید و تبادل اطلاعات نهاد ریاست جمهوری اسلامی‌ایران بر پایه این استاندارد، یک پروفایل حفاظتی معرفی کرده است که در حال حاضر با عنوان پروفایل حفاظتی برنامه‌های کاربردی تحت شبکه با نسخه 1.1 مربوط به اردیبهشت 96 از طریق پرتال اداره کل ارزیابی محصولات این معاونت در اختیار عموم قرار گرفته است. تلاش می‌کنیم تا بخش‌های مختلف الزامات امنیتی ارائه شده در این پروفایل را بررسی کنیم.

پروفایل حفاظتی برنامه های کاربردی تحت شبکه

این پروفایل حفاظتی مجموعه قابلیت‌هایی را معرفی می‌کند که هر نرم‌افزار تحت وب (به عنوان نوعی از نرم‌افزارهای تحت شبکه) باید برای امن کردن خود، این الزامات را رعایت کرده باشد. این پروفایل حفاظتی با وام داری از کلاس‌بندی‌های استاندارد معیار

مشترک،الزامات را مشخص کرده است.در ادامه، این کلاس‌بندی‌ها و خلاصه‌ای از نوع الزاماتی که در هر کلاس وجود دارد را بیان می‌کنیم:

- **کلاس ممیزی امنیت:**

در رویکرد کشف رویدادها بر اساس توضیحات داده شده نگهداری تاریخچه رویدادها الزامی‌ست. در این کلاس، مجموعه‌ای از الزامات آورده شده که مشخص می‌کنند، اطلاعات ممیزی چگونه باید تولید شوند، حاوی چه اطلاعاتی باشند، چگونه باید گزارشگیری یا ذخیره شوند و یا مدیریت آنها چگونه است. در این کلاس سعی شده است که با استفاده از الزامات تعریف شده، چرخه حیات کامل اطلاعات ممیزی (لاگ‌ها) به صورت یکپارچه از تولید تا امحاء، معرفی و امنیت آنها تامین شود.

2-کلاس پشتیبانی از رمزنگاری:

در این کلاس، الزاماتی آورده شده است که طی آن مشخص می‌شود محصول باید از چه الگوریتم‌های رمزنگاری و درهم‌ساز برای ایجاد امنیت در سایر الزامات استفاده کند.

3-کلاس شناسایی و احراز هویت:

در این کلاس، الزاماتی در حوزه احراز هویت تعریف شده که این عملیات را امن می‌کند. شباهت‌های بسیاری بین این کلاس با قابلیت‌های مورد نیاز طبقه‌بندی احراز هویت در استاندارد ASVS وجود دارد. هر دو برای امن کردن احراز هویت، مجموعه‌ای از قابلیت‌ها مانند احراز هویت دو عاملی، شیوه‌های جلوگیری از حملات DDos بر روی کلمه عبور و ... را پشتیبانی می‌کنند.

4-کلاس حفاظت از داده‌های کاربری:

داده‌های کاربری یا همان اطلاعاتی که نرم‌افزار، مسئول مدیریت آن در کسب و کار های مختلف است در این کلاس، محافظت می‌شوند؛ البته این الزامات به معنای ایجاد مفهوم داده‌های قابل اطمینان و همچنین مفهوم دسترسی‌ها به اطلاعات است. الزامات این کلاس، قابلیت‌هایی را درخواست می‌کند تا اطلاعات در اختیار افراد مجاز قرار گیرند و هرگونه ورود و خروج اطلاعات به یا از نرم‌افزار با ساختارهایی مثل امضای دیجیتال مطمئن شوند. الزاماتی در رابطه با کشف تغییرات غیرمجاز در داده‌ها معرفی می‌کند که بتواند داده‌های مطمئن و نامطمئن را از یکدیگر تفکیک کند. در مورد دسترسی‌ها به اطلاعات نیز الزاماتی در این کلاس آورده شده است تا تعریف خط مشی دسترسی به آنها در نرم‌افزار مشخص و کنترل شود.

5-کلاس مدیریت امنیت:

در این کلاس، مجموعه قابلیت‌هایی آورده شده که به عنوان قابلیت‌های امنیتی در اختیار مدیران قرار می‌گیرد. آنها با استفاده از این تنظیمات می‌توانند سیاست‌های امنیتی خود را در نرم‌افزار اعمال کنند.

6-کلاس حفاظت از توابع امنیتی محصول:

توابع امنیتی محصول، مجموعه‌ای از توابعی است که در اختیار اجزای مختلف محصول یا سایر نرم‌افزارها و یا کاربران قرار دارند. در این کلاس، الزاماتی آورده شده‌اند تا از این توابع محافظت شود. این الزامات خطاهای شکست، انتقال داده‌ها بین اجزای

مختلف یا بین نرم‌افزار دیگری با نرم‌افزار در حال آزمون را مشخص می‌کند. همچنین الزاماتی را در رابطه با مفاهیم مُهر زمانی بر روی داده‌ها برای اطمینان به آنها و شیوه‌هایی نیز برای بروزرسانی نرم‌افزار ارائه می‌دهد.

7-کلاس دسترسی به محصول:

در این کلاس، الزاماتی درباره شیوه برقراری ارتباط بین کاربر و نرم‌افزار تعریف شده است که با توجه به بستر وب بودن نرم‌افزار در این پروفایل حفاظتی الزامات مربوط به نشست بین کاربر و نرم‌افزار را مشخص می‌کند. در این کلاس الزاماتی در رابطه با محدودیت تعداد نشست‌های همزمان، شیوه برقراری و خاتمه و همچنین نگهداری سوابق نشست‌ها معرفی شده که برای مدیریت نشست‌ها توسط کاربران است. برخی از این الزامات با استاندارد ASVS مشابه است.

8-کلاس تخصیص منابع:

در این کلاس، الزاماتی در رابطه با تحمل خطا برای نرم‌افزار معرفی شده است.

9-کلاس کانال‌ها/مسیرهای مورد اعتماد:

در این کلاس، الزاماتی در رابطه با ایجاد اطمینان در خطوط انتقال اطلاعات معرفی شده است. این الزامات می‌گویند که از چه پروتکل‌های امنی باید برای استفاده در انتقال اطلاعات در نرم‌افزار استفاده شود.

مجموعه این کلاس‌ها سعی دارند الزاماتی را معرفی کنند که سطح اطمینان به اطلاعات

را افزایش دهد. این الزامات نیز کاملا در رابطه با اطمینان به اطلاعات نیست و گاهی ناگزیر شده است علاوه بر کشف اطلاعات نامطمئن الزاماتی را نیز برای پیشگیری از بعضی از حملات داشته باشد. ولی رویکرد اصلی این استاندارد، کشف رویدادها و تفکیک اطلاعات نامطمئن و مطمئن است.

استاندارد معیار مشترک سعی می‌کند تا جای ممکن با تاثیری که بر روی روند خط تولید محصولات امن دارد به امنیت نرم‌افزار کمک کند؛ اما این استاندارد نقاط ضعف و قدرت خود را دارد که در این باره کمی‌توضیح می‌دهیم.

نقاط ضعف معیار مشترک

این استاندارد برای تمامی‌انواع سیستم‌ها و محصولات کامپیوتری ایجاد شده و از این رو به سطحی از انتزاع رسیده است که هر بند از آن، نیازمند تفسیرهای مختلف است. این انتزاع باعث شده که حتی پروفایل‌های حفاظتی که برای نوع‌های مختلف ایجاد می‌شود نیز به سطحی از انتزاع برسد که نیاز به تفسیر داشته باشند. معمولا این تفاسیر باعث ایجاد چالش‌های بزرگی بین آزمایشگاه‌ها، تولیدکنندگان محصولات و دولت‌ها می‌شوند.

هدف الزامات آورده شده در پروفایل‌های حفاظتی، برآورده کردن نیازمندی‌های اعلام شده در استاندارد است که رویکرد امنیتی را بر مبنای امن‌سازی تولید هدف‌گذاری کرده است. همین امر موجب شده این استاندارد هرچقدر برای امنیت محصولاتی بر پایه علوم کامپیوتری مانند سیستم عامل‌ها و پایگاه داده‌ها موثر است برای نرم‌افزارهای بستر وب کم اثر باشد.

این استاندارد تضمینی برای امنیت ارائه نمی‌دهد اما می‌تواند این اطمینان را ایجاد کند که ادعاهای امنیتی اعلام شده توسط تولیدکنندگان محصول به صورت مستقل تست و صحت انجام آن‌ها تایید شوند. درنرم‌افزارهای بستر وب این استاندارد باعث جلوگیری از شیوه‌های حمله نمی‌شود بلکه می‌تواند اگر حمله‌ای صورت گرفت آن را کشف و اطلاعات تحت تاثیر حمله را از سایر اطلاعات مطمئن تفکیک کند.

این استاندارد برای تولیدکنندگان، بسیار هزینه‌بر و زمان‌بر است. رسیدن به سطوح سه یا چهار این استاندارد حجم زیادی از منابع مالی و زمانی شرکت‌های تولید کننده را درگیر خود می‌کند و در دنیای وب این هزینه‌ها (همانطور که صحبت شد) تضمین‌کننده امنیت نرم‌افزار نیستند.

نقاط قوت معیار مشترک

این استاندارد می‌تواند تعاریف امنیت در هر محصول یا سیستم کامپیوتری را مشخص کند و سنجه‌ای برای تمامی آنها باشد.از این‌رو اکثر دولت‌ها به دنبال استفاده از این استاندارد برای صدور گواهینامه‌های امنیتی تمامی محصولات دنیای IT هستند.

این استاندارد برای استفاده‌کنندگان نیز می‌تواند مفید باشد. آن‌ها می‌توانند مستندات ادعایی مربوط به تمامی نیازمندی‌های امنیتی خود را اعم از نرم‌افزاری و سخت‌افزاری با یک معیار ثابت بسنجند و بر این اساس از محصولات و سیستم‌های دارای یک معیار مشترک استفاده کنند. این استاندارد همچنین می‌تواند برای مهندسی امنیت در محصولات IT، نقش یک متدولوژی را نیز بازی کند و در کنار متدولوژی های رایج تولید نرم‌افزار کمک کند تا بر اساس یک روش شناسی مناسب رویکردهای امنیتی را به

صورت فرآیندهایی استاندارد در شرکت‌ها جا انداخت.

سنجش تاثیر معیار مشترک بر امنیت نرم‌افزارهای وب

اگر بخواهم صرفا با نگاه نرم‌افزارهای وب، این استاندارد را بسنجم باید بگویم که این استاندارد برای نرم‌افزارهای وبی هزینه‌بر و ناکارآمد است و نمی‌توان این‌گونه نرم‌افزارها را با استفاده از این استاندارد امن کرد. به عنوان کسی که برای تمامی‌الزامات پروفایل حفاظتی در نرم‌افزار یا در طراحی قابلیت یا در معماری و یا در پیاده سازی الزامات دخیل بوده‌ام به جرات می‌توانم بگویم که صرفا تکیه بر این استاندارد به منظور امن‌سازی نرم‌افزارهای وب، ایجاد امنیت در نرم‌افزار را با شکست بزرگی مواجه خواهد کرد؛ البته این جمله به این معنی نیست که این استاندارد نتواند برای امنیت نرم‌افزارهای وب مناسب باشد بلکه به این معنی است که نمی‌توان فقط با تکیه بر این استاندارد تمامی امنیت مورد نیاز نرم‌افزارهای وبی را تامین کرد.

شیوه امن سازی نرم‌افزارهای تحت وب در شرکت‌های تولید کننده نرم افزار

شرکت‌های تولیدکننده نرم‌افزار باید چه شیوه‌ای را در بحث امن‌سازی نرم‌افزارهای وب تولیدی خود پیش بگیرند؟ چگونه باید بحث امنیت در بخش‌های مختلف شرکت‌های نرم افزاری جاری شود؟ چه روشی برای تولید امنیت در نرم‌افزار می‌توان استفاده کرد؟ این سوالات بسیار برای شرکت‌های نرم‌افزاری حائز اهمیت است و باید به خیلی از مسائل

از جمله هزینه‌ها، مزایا و سطوح امنیت و ... پرداخت. پاسخ‌های هر شرکت به این سوال‌ها به ایجاد یک استراتژی برای تولید نرم‌افزار منجر خواهد شد.

در ابتدا باید دانست که امنیت برای نرم‌افزارهای وب بیشتر از اینکه یک مجموعه تکنیک‌های فنی باشد یک فرهنگ سازمانی است. تمامی افراد دخیل در جای‌جای فازهای تولید نرم‌افزار از نیازسنجی تا استقرار و پشتیبانی نرم‌افزار درگیر بحث امنیت خواهند بود و باید استراتژی مشخصی برای ایجاد این فرهنگ در سازمان‌ها وجود داشته باشد. این استراتژی می‌تواند حاوی بخش‌های زیر باشد:

1-آموزش امنیت

2-انتخاب یا تولید نقشه راه برای امنیت

3-راهنمایی برای شیوه اجرای امنیت

4-راهنمایی برای شیوه آزمودن تاثیر امنیت

در رابطه با آموزش امنیت شرکت‌های تولیدکننده نرم‌افزار باید تمامی افراد درگیر در فرآیند تولید را چه از لحاظ فرهنگی و چه از لحاظ فنی آموزش دهند. در رابطه با بعد فرهنگی امنیت باید به تمامی افراد اهمیت آن را آموزش داد ولی به ازای هر بخش یا تیم باید این اهمیت هدف‌گذاری شود. به عنوان مثال اهمیت امنیت برای واحد فروش یک شرکت، تعریفی متفاوت با اهمیت امنیت برای افراد درگیر در واحد تولید نرم‌افزار دارد و باید در شرکت‌های نرم‌افزار این تفاوت‌ها درک شود و هر یک از بخش‌ها را بر اساس نیاز آموزش داد. آموزش در بعد فنی نیز باید سطح‌بندی شود، کارشناس تولید نرم‌افزار

باید دانشی از شیوه‌های حمله، روش‌های جلوگیری از آن و شیوه‌های تست امنیت را دارا باشد؛ اما کارشناس استقرار به دانستن شیوه‌های تنظیم نرم‌افزار برای جلوگیری از حملات، نیاز دارد. این آموزش‌ها باید به وسیله نقشه راهی هدفمند برای افراد انجام شود تا بتوان بهترین نتیجه را گرفت. شاید بهترین حالت در آموزش این باشد که ارتقای سمت‌های کارشناسان در شرکت‌های تولید نرم‌افزار علاوه بر عناصر دیگر به ارتقای دانش افراد در زمینه امنیت نیز وابسته شود.

شرکت‌های نرم افزاری باید حتما برای امنیت نرم‌افزارهای تولیدی خود نقشه راهی انتخاب و یا تولید کنند. پیشنهاد من استفاده از استاندارد ASVS برای تولید نرم‌افزارهای تحت وب است. این استاندارد سبک است و شفافیت لازم برای یکپارچه سازی مفاهیم را همراه با ابزار ها و راهنماهای مناسب شرکت‌های تولیدکننده نرم‌افزار را دارا است و نقشه راه بسیار مناسبی‌ست. این استاندارد نیاز به قابلیت‌هایی دارد تا نه تنها امنیت با شیوه پیشگیری جلوی هر حمله‌ای را بگیرد؛ بلکه اجازه مدیریت امنیت برای استفاده‌کنندگان نرم‌افزار را فراهم کند. از این رو انتخاب بعضی از الزامات استاندارد معیار مشترک و پیاده‌سازی آن‌ها این کمک را می‌کند که بتوان نرم افزاری کامل‌تر در زمینه مدیریت امنیت نرم‌افزار ارائه داد.

هر شرکت نرم‌افزاری همچنین به راهنمایی برای شیوه اجرای امنیت نیاز دارد. این راهنما مجموعه‌ای از فرآیندهایی که باید در حوزه امنیت اجرا شود را مشخص می‌کند و نیازمندی‌های مربوط به هر فاز را شامل می‌شود. به عنوان مثال این راهنما مشخص می‌کند در فاز طراحی چگونه باید امنیت در طراحی‌ها اجرا شود و چگونه باید در جلسات بازنگری طراحی، مشکلات امنیتی آنها کشف و به عنوان باگ طراحی رفع شود.

در مجموع باید این راهنما امنیت را در فازهای نیازسنجی، تحلیل، طراحی و معماری، پیاده‌سازی، تست، استقرار و پشتیبانی نرم‌افزار تعریف کند و راهکارهایی در هر یک از این فازها برای اجرا و برای بررسی سطح اجرا در بازنگری ارائه دهد. همچنین باید امنیت در مدیریت نرم‌افزار توسط ریسک‌های امنیتی در مدیریت ریسک‌ها حضور یابد تا بتوان ریسک‌های امنیتی تولید نرم‌افزار را نیز برای جلوگیری از وقوع پیگیری کرد؛ بنابراین نیاز به تعریف متریک‌هایی برای پیگیری‌کردن میزان امنیت نرم‌افزار وجود دارد و این متریک‌ها باید در فرایندهای تولید تا تست نرم‌افزار تعریف و اطلاعات آن‌ها جمع شود تا بتوان برای هر نسخه دانست که میزان امنیت هر نسخه، چقدر است.

واحدهای تست تیم‌های تولیدکننده در بحث امنیت نقش کلیدی در آزمودن تاثیرات تمامی‌کارهای انجام شده بر روی امنیت نرم‌افزار را دارند. این کارشناسان باید تمامی زوایای مختلف تست امنیت را بشناسند و بتوانند به صورت جعبه سیاه انواع حملات را بر روی نرم‌افزار تست کنند. از این رو شیوه ای برای آزمودن امنیت نرم‌افزار نیاز است تا این افراد طی آن تمامی راه‌های نفوذ نرم‌افزار را پیش از انتشار نسخه برای استفاده‌کنندگان پیدا کنند تا راه‌های نفوذ بسته شود.

نتیجه‌گیری

ما در بخش اول امنیت را تعریف و بعد از آن در بخش دوم رویکرد پیشگیری و در این بخش رویکرد کشف رویدادها را بررسی و بر اساس آن‌ها تفکیکی بین وظایف تولیدکنندگان و مصرف‌کنندگان ارائه دادیم. در انتها نیز با نگاه به شرکت‌های تولیدکننده نرم‌افزار شیوه‌ای ارائه شد تا اینگونه شرکت‌ها بدانند در زمینه امن‌سازی نرم‌افزار چه

رویکردی می‌توانند اتخاذ کنند.

باید بدانیم که امنیت بخشی جداناپذیر از نرم‌افزارهای وب است و شرکت‌های تولیدکننده نرم‌افزار باید برای ایجاد امنیت نرم‌افزار تلاش و هزینه کنند؛ زیرا اعتماد یک اصل مهم در دنیای نرم افزارهاست. امنیت در دنیای وب جدا از بحث‌های فنی مستلزم تعریفی فرهنگی است تا هم تولیدکنندگان و هم استفاده‌کنندگان از مزیت‌های آن سود ببرند. استفاده‌کننده باید مطالبات امنیتی داشته باشد و تولیدکننده باید مطالبات را پاسخگو باشد. با توجه به خدمات بسیار زیادی که در حال حاضر به صورت نرم‌افزارهای مختلف در بستر وب ارائه می‌شود امنیت این نرم‌افزارها بسیار حائز اهمیت است. در ایران با توجه به نوپا بودن این بحث طی چهار ـ پنج سال گذشته ما سازندگان این فرهنگ خواهیم بود و بسیار مهم است که این فرهنگ به شیوه درستی ایجاد شود. تولیدکنندگان نرم‌افزار در حال حاضر با توجه به دانش فنی بحث امنیت می‌توانند فرهنگ‌سازان خوبی در این زمینه باشند و حتی خدمات آموزشی امنیتی را به استفاده‌کنندگان خود دهند تا این فرهنگ به شیوه مطلوبی ایجاد شود.

تولیدکنندگان نرم‌افزارهای ایرانی هرچقدر در زمینه دانش فنی و فرهنگی امنیت ارتقاء یابند، سطح امنیت جامعه استفاده‌کننده از این نرم‌افزارها افزایش خواهد یافت.

بخش پایانی