به نام خدا

طرح ارزیابی امنیتی محصولات

مرکز مدیریت راهبردی افتا

مهر ۹۳

نسخه ۱,۰

پیشگفتار

با رشد روز افزون تهدیدات در فضای تولید و تبادل اطلاعات، مسئله امنیت جایگاه ویژه‌ای پیدا نموده است. یکی از مهمترین دغدغه‌های امنیتی بدین جهت تولیدکنندگان محصولات فضای تولید و تبادل اطلاعات، سعی در تولید محصولاتی دارند که با تهدیدات موجود مقابله نماید.

«طرح ارزیابی امنیتی» ذی‌نفعان این حوزه را مشخص کرده و ساختار، فرایندها، روال‌ها، نقشها، تعاملات و ارتباطات فی مابین را شرح می‌دهد.

فهرست

مقدمه

در راستای اجرایی سازی اقدام سوم از راهبرد دوم سند افتا در ارزیابی امنیتی محصولات فتا، «طرح ارزیابی امنیتی» جهت ساماندهی ارزیابی امنیتی محصولات فتا مبتنی بر استاندارد ارزیابی امنیتی معیار مشترک[1] و سایر استانداردها و دستورالعمل‌های ابلاغی از سوی مرکز افتا تهیه گردیده است. هدف از «طرح ارزیابی امنیتی»، ارائه راهکار و نقشه راه ارزیابی محصولات فضای تولید و تبادل اطلاعات (فتا) و صدور گواهی برای آنها براساس استاندارد ارزیابی امنیتی معیار مشترک و سایر استانداردها و دستورالعمل‌های ابلاغی مرکز افتا می‌باشد، تا مصرف کنندگان نسبت به برآورده شدن نیازهای امنیتی خود اطمینان حاصل نمایند و تولید کنندگان در مسیر اقدام به ارتقاء امنیت محصولات خود گام بردارند. این سند برای ارائه یک دید کلی و توصیف وظایف مرکز افتا و سازمان، تولیدکننده، آزمایشگاه و مصرف کننده محصولات ارزیابی شده در نظر گرفته شده است و شامل چهار فصل اصلی به شرح ذیل می‌باشد:

فصل اول، به معرفی اصطلاحات و تعاریف پرداخته و اهداف طرح ارزیابی امنیتی و اسناد مرتبط را شرح می‌دهد.
فصل دوم دیدکلی از طرح ارزیابی امنیتی و شرح خلاصه‌ای از فعالیت‌های اصلی آن را ارائه داده و نقش‌های اصلی در طرح ارزیابی امنیتی که در ارزیابی امنیتی محصولات فتا مشارکت دارند، همچون مرکز افتا، سازمان، آزمایشگاه و تولیدکننده محصول و مصرف کننده را معرفی می‌نماید.
فصل سوم فرایند ارزیابی امنیتی محصولات فتا را شرح می‌دهد و تعاملات و ارتباطات ذی نفعان را تبیین می‌کند.
فصل چهارم به نظارت بر ارزیابی امنیتی می‌پردازد.
فصل پنجم نیز به مدیریت گواهی اختصاص یافته است.

۱ کلیات

۱,۱ معرفی اصطلاحات

- **فتا**: فضای تولید و تبادل اطلاعات
- **مرکز افتا** : مرکز مدیریت راهبردی افتا ریاست جمهوری.
- **سازمان** : سازمان فناوری اطلاعات
- **استاندارد ارزیابی امنیتی معیار مشترک (ISO 15408 Common Criteria)**

استاندارد معیار مشترک یا ISO 15408 استانداردی برای ارزیابی امنیتی محصولات می‌باشد.

[1] ISO 15408 (Common Criteria)

- **هدف ارزیابی (TOE[۲])**

به محصول یا کارکرد مورد ارزیابی براساس «استاندارد ارزیابی معیار مشترک»، هدف ارزیابی گفته می‌شود. در این سند منظور از محصول همان هدف ارزیابی است.

- **متدلوژی ارزیابی معیار مشترک (Common Evaluation Methodology)**

متدلوژی برای ارزیابی امنیتی محصولات فتا می‌باشد که از یک سند فنی تشکیل شده و روش‌های ارزیابی امنیتی را شرح می‌دهد.

- **طرح ارزیابی امنیتی (Security Evaluation Scheme)**

طرح ارزیابی امنیتی سندی است که توسط مرکز افتا و سازمان ارائه می‌شود و دیدکلی از روال‌ها و خط‌مشی‌ها و راهبردهای ارزیابی امنیتی ارائه می‌نماید.

- **آزمایشگاه (Laboratory)**

آزمایشگاه ارزیابی امنیتی محصولات فتا

- **تولید کننده (Developer)**

تولید کننده محصول و یا متقاضی ارزیابی محصول

- **ارزیاب (Evaluator)**

کارمند آزمایشگاه که وظیفه‌ی ارزیابی محصول را دارد.

- **پروفایل حفاظتی (PP[۳])**

بیانیه‌ای مستقل از پیاده سازی الزامات امنیتی برای یک نوع محصول – نه یک محصول خاص-، که الزامات امنیتی را به صورت کلی بیان می‌دارد.

- **هدف امنیتی (ST[۴])**

بیانیه‌ای از الزامات امنیتی وابسته به پیاده سازی، برای یک هدف ارزیابی مشخص، که الزامات امنیتی را به صورت جزئی‌تر بیان می‌دارد. به عبارت دیگر مجموعه ای از نیازمندی‌ها و ویژگیهای امنیتی یک محصول (هدف مورد ارزیابی)، که به عنوان مبنای ارزیابی آن مورد استفاده قرار می‌گیرد.

- **کارکرد امنیتی (Security Functionality)**

عملکرد امنیتی محصول در زمینه ممیزی امنیت، رمزنگاری، شناسایی و احرازهویت، مدیریت دسترسی‌ها، حفاظت از داده‌ها و اطلاعات و غیره، کارکرد امنیتی نامیده می‌شود.

- **طرح کار ارزیابی (Evaluation Work Plan)**

---

[۲] Target Of Evaluation

[۳] Protection Profile

[۴] Security Target

سندی است که توسط آزمایشگاه تولید می‌شود و جزئیات فعالیت‌های برنامه ریزی شده و زمانبندی آنها را برای ارزیابی امنیتی محصولات فتا مشخص می‌کند.

- **گزارش اعتبارسنجی (Validation Report)**

سندی است که پس از پایان ارزیابی و تأیید مرکز افتا، توسط سازمان منتشر می‌شود و در برگیرنده خلاصه‌ای از نتایج ارزیابی امنیتی است.

- **سطح اطمینان ارزیابی (Evaluation Assurance Level)**

بسته‌ای از نیازهای حصول اطمینان استاندارد ارزیابی معیار مشترک است که معیار اطمینان از پیش تعریف شده آن را نشان می‌دهد. این استاندارد ۷ سطح سلسله مراتبی از ۱ تا ۷ تعریف می‌کند.

- **مصرف کننده**: منظور از مصرف کننده حوزه ای است که محصول در آن مورد استفاده قرار گرفته و بکارگرفته می‌شود.
- **اعتباربخشی:** بررسی وجود الزامات تعیین شده برای احراز اعتبار آزمایشگاه جهت ارزیابی محصول بر اساس ضوابط و مقررات تعیین شده از سوی افتا و صدور گواهی مجوز فعالیت در این حوزه بر اساس طرح ارزیابی امنیتی
- **اعتبارسنجی**: انجام نظارت بر فرایند ارزیابی و ایجاد اطمینان از صحت نتایج و روالها

۲,۱ اهداف طرح ارزیابی امنیتی

نگرانی‌های امنیتی سبب شده تا تولیدکنندگان محصولات در صدد ارتقاء امنیت محصولاتشان برآیند. همچنین مصرف کنندگان در هنگام انتخاب محصول مورد نظر با طیف وسیعی از محصولات با قابلیت‌ها و محدودیت‌های متفاوت رو به رو هستند. برای آنها مسئله مهم انتخاب محصولی است که بتواند نیازهای مصرف کننده را برآورده نماید و از اطلاعات آنها در حد مناسبی محافظت نماید.

به منظور کمک به مصرف کننده در انتخاب محصولی که نیازهای امنیتی‌اش را برآورده نماید و کمک به سازنده محصول در مقبول واقع شدن در داخل کشور و بازارهای جهانی، بر اساس استاندارد ارزیابی معیار مشترک و سایر استانداردها و دستورالعمل‌های ابلاغی مرکز افتا، «طرح ارزیابی امنیتی» توسط مرکز افتا و سازمان تدوین گردیده است. در ادامه به مفهوم طرح ارزیابی امنیتی معیار مشترک پرداخته خواهد شد. آنچه که در این سند ارائه شده دیدگاه کلی از طرح ارزیابی امنیتی بوده که برای اطلاع از جزئیات این طرح به دیگر اسناد تهیه شده مرتبط که در بند ۱-۳ این سند معرفی شده، مراجعه شود.

اهداف اصلی از ایجاد «طرح ارزیابی امنیتی» عبارتند از:

- حصول اطمینان از انجام ارزیابی امنیتی محصولات فتا منطبق بر استاندارد ارزیابی معیار مشترک و قابل دسترس، تکرارپذیر و امتحان پذیر بودن ارزیابی

- رفع مخاطرات و دغدغه‌های امنیتی ناشی از بکارگیری محصولات ارزیابی نشده
- برآوردن نیازهای صنعت و دولت برای ارزیابی محصولات فتا با هزینه منطقی
- بهبود دسترس‌پذیری محصولات فتای ارزیابی شده
- حمایت از ایجاد و توسعه آزمایشگاه‌های ارزیابی امنیتی
- حمایت از توسعه بومی سازی محصولات فتا

۳,۱ سندهای مرتبط

سندهای مرتبط با طرح ارزیابی امنیتی که توسط مرکز افتا تدوین می‌شوند عبارتند از:

سند ۱: طرح ارزیابی امنیتی

سند ۲: نظامنامه کیفیت

سند ۳: راهنمای اعتبارسنج

سند ۴: راهنمای آزمایشگاه‌های ارزیابی امنیتی محصولات فتا

سند ۵: راهنمای تولیدکننده

سند ۶: تداوم گواهی: راهنمایی برای نگهداری و ارزیابی مجدد

سند ۷: راهنمای نوشتن پروفایل حفاظتی/سند هدف امنیتی

سند ۸: راهنمای اعتباربخشی آزمایشگاه‌ها

۲ دیدکلی طرح ارزیابی امنیتی

در ارزیابی امنیتی محصولات، نهادهای مختلفی شرکت دارند تا بتوان این طرح را پیاده سازی نمود. ذی‌نفعان اصلی در طرح ارزیابی امنیتی عبارتند از:

- تولید کننده
- آزمایشگاه
- مرکز افتا
- سازمان
- مصرف کننده

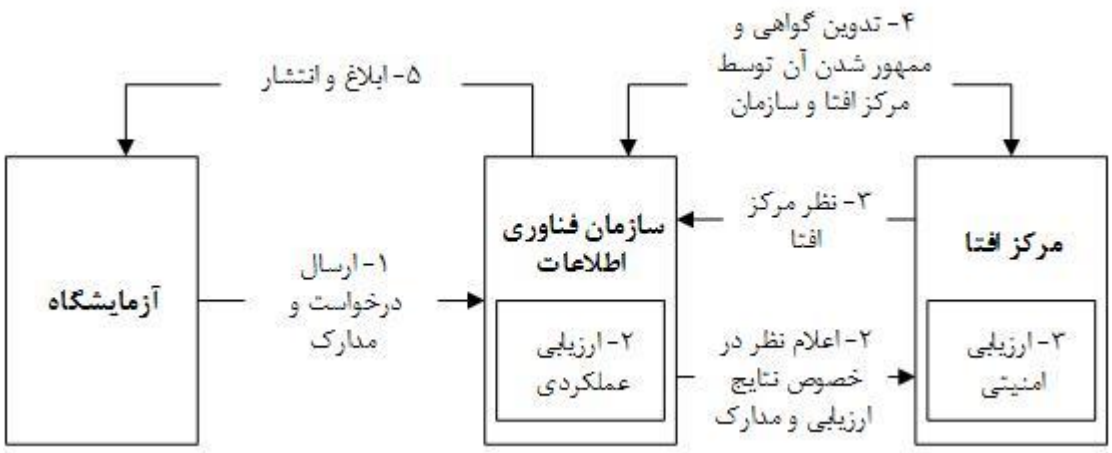
در ادامه وظایف و مسئولیت‌های هر یک از این پنج نهاد شرح داده می‌شود.

۱,۲ تولید کننده

تولیدکننده یک نهاد دولتی، خصوصی است و یا سازمانی می‌باشد که خواستار ارزیابی امنیتی محصول خود است و هزینه مالی آن را تقبل می‌کند. تولید کننده باید تمام مدارک مورد نیاز جهت ارزیابی محصول را در اختیار آزمایشگاه قرار دهد. برای اطلاع بیشتر از نقش و وظایف تولیدکننده محصول در طول روال ارزیابی به سند «راهنمای تولیدکننده» مراجعه شود.

۲,۲ آزمایشگاه‌های ارزیابی امنیتی محصولات فتا

آزمایشگاه‌های ارزیابی در فرایند ارزیابی امنیتی محصولات نقش بسیار مهمی دارند. صرفاً آزمایشگاه‌هایی در این فرایند شرکت می‌کنند که توسط مرکز افتا و سازمان مطابق شکل (۱) اعتبارسنجی[۵] و اعتباربخشی[۶] شده و گواهی انجام فعالیت دریافت کرده باشند. در شکل شماره (۱) فرایند اعتبار بخشی آزمایشگاه نشان داده شده است.



شکل ۱: فرایند اعتباربخشی آزمایشگاه

همانگونه که در شکل شماره (۱) نشان داده شده است، فرایند دریافت گواهی آزمایشگاه عبارت است از:

[۵] - Validation

[۶] -Accreditation

۱. ارسال درخواست و مدارک از سوی آزمایشگاه به سازمان فناوری اطلاعات
۲. ارزیابی عملکردی آزمایشگاه توسط سازمان و اعلام نظر در خصوص نتایج ارزیابی و مدارک و اعلام به مرکز افتا
۳. ارزیابی امنیتی آزمایشگاه توسط مرکز افتا
۴. جمع بندی نتایج ارزیابی‌ها توسط مرکز افتا و اعلام به سازمان
۵. صدور گواهی بر اساس نتایج بند ۴ توسط سازمان و مرکز افتا به صورت مشترک

آزمایشگاه‌هایی که گواهی دریافت می‌کنند باید الزامات زیر را برآورده نمایند:

- الزامات مطرح شده در سند «راهنمای اعتباربخشی آزمایشگاه»
- موارد مطرح شده در تعهدنامه اخذ شده از آزمایشگاه
- دارا بودن معیارهای مشخص شده برای ارزیابی امنیتی و دیگر الزامات طرح ارزیابی امنیتی تعریف شده که توسط مرکز افتا در سند «راهنمای آزمایشگاه‌ها» مطرح شده است
- تأمین امنیت فناوری اطلاعات و ارتباطات آزمایشگاه و حفاظت از اطلاعات مرتبط با ارزیابی امنیتی محصولات
- انجام ارزیابی امنیتی بر اساس استانداردها، آیین نامه‌ها، مقررات و ضوابط ابلاغی مرکز افتا
- پایبندی به شرایطی که بر اساس آنها اعتبار بخشی شده است
- ارائه گزارشات و نتایج ارزیابی امنیتی محصولات صرفاً به مرکز افتا و تولید کننده
- رعایت انصاف و بی طرفی و حفظ استقلال آزمایشگاه
- انجام ارزیابی امنیتی در حداقل زمان ممکن
- .....

آزمایشگاه برای ارزیابی امنیتی محصولات و پروفایل حفاظتی، بر اساس ابلاغیه «راهنمای عقد قرارداد ارزیابی امنیتی محصول» با تولید کننده، قرارداد منعقد می‌نماید. ارزیابی امنیتی محصولات منطبق بر روال‌ها و خط‌مشی‌های طرح ارزیابی امنیتی انجام می‌شود.

آزمایشگاه باید بالاترین استانداردهای بی‌طرفی، صحت و محرمانگی را رعایت نماید و در چارچوب طرح ارزیابی امنیتی عمل نماید. با توجه به محرمانگی، آزمایشگاه باید دارای روال‌ها و خط‌مشی‌های مستند شده جهت اطمینان از حفاظت اطلاعات حساس و نتایج ارزیابی‌ها باشد. این روال‌ها باید توسط مرکز افتا ممیزی شده و مورد نظارت مستمر قرار گیرد.

آزمایشگاه نباید محصولاتی را که مالک آن در آزمایشگاه منافعی دارد، ارزیابی نماید. همچنین تیم ارزیابی یک محصول /پروفایل حفاظتی نباید تحت هیچ شرایطی درگیر مسائل زیر شوند:

- توسعه و ارزیابی همزمان آن محصول

- ارائه خدمات مشاوره‌ای به تولید کننده آن محصول یا پروفایل حفاظتی

آزمایشگاه باید اطمینان دهد در فرایند ارزیابی امنیتی محصول یا پروفایل حفاظتی، بر اساس انصاف و بی طرفی عمل می‌نماید. در صورت وجود چنین مشکلی (منصفانه نبودن ارزیابی و دخیل نمودن منافع)، مرکز افتا باید در این مورد تصمیم‌گیری نموده زیرا ممکن است صحت ارزیابی امنیتی محصول تهدید گردد.

۳,۲ مرکز افتا

به عنوان یک نهاد دولتی بالاترین سطح در استاندارد ارزیابی معیار مشترک است که آزمایشگاه‌ها را اعتبار بخشی نموده و به همراه سازمان گواهی فعالیت آزمایشگاه را صادر می‌نماید (مطابق شکل شماره ۱) و منطبق بودن آزمایشگاه‌های ارزیابی امنیتی بر روال‌ها و خط‌مشی‌های این مرکز را بررسی می‌نماید. مرکز افتا برای آزمایشگاه‌های ارزیابی راهنمای فنی ارائه نموده و حین و پس از ارزیابی آزمایشگاه، انطباق نتایج ارزیابی امنیتی محصولات فتا را با استاندارد ارزیابی معیار مشترک تائید می‌نماید و محصولات ارزیابی شده توسط آزمایشگاه را جهت صدور گواهی به سازمان معرفی می‌نماید. هدف اصلی مرکز افتا اطمینان از اعتبار ارزیابی و خدمات اعتبارسنجی برای حوزه مصرف می‌باشد. مرکز افتا در صورت لزوم می‌تواند روال‌ها و خط‌مشی‌ها را تفسیر و اصلاح نماید.

هرگونه اختلافی که از سوی یکی از بخش‌های درگیر در فرایند ارزیابی مطرح شود (تولید کننده محصول یا آزمایشگاه و مصرف کننده) باید برای حل و فصل توسط سازمان به این مرکز ارجاع داده شود.

به طور کلی مسئولیت مرکز افتا عبارت است از:

- تهیه و تدوین آیین نامه‌ها، دستورالعمل‌ها، مقررات، فرایندها، روال‌ها و خط‌مشی‌ها برای «طرح ارزیابی امنیتی»، و اطمینان از پیاده‌سازی آن‌ها
- تائید و اعتبار بخشی آزمایشگاه‌ها و اطلاع رسانی به سازمان
- نظارت بر آزمایشگاه‌ها جهت اطمینان از تبعیت آن‌ها از استانداردها، آیین نامه‌ها و دستورالعمل‌ها، روال‌ها و خط مشی‌ها و متدلوژی ارزیابی و پروفایل‌های حفاظتی ابلاغی توسط مرکز افتا
- لغو گواهی در صورت برآورده ننمودن شرایط طرح ارزیابی امنیتی توسط آزمایشگاه‌ها و اطلاع رسانی به سازمان
- اطمینان از وجود روال‌های مناسب در «طرح ارزیابی امنیتی» و پیروی از آن‌ها برای حفاظت از اطلاعات حساس مرتبط با محصولات یا پروفایل‌های حفاظتی تحت ارزیابی
- ارائه پیشنهادات، راهنمایی‌ها، پشتیبانی‌های لازم و استانداردهایی برای آموزش آزمایشگاه‌ها در صورت نیاز

- بررسی گزارشات فنی ارزیابی آزمایشگاه‌ها و حصول اطمینان از سازگاری نتایج به دست آمده با مدارک ارائه شده و اعمال درست استاندارد ارزیابی معیار مشترک و سایر استانداردها، دستورالعمل‌ها و متدلوژی ارزیابی
- اطمینان از سازگاری ارزیابی آزمایشگاه با طرح ارزیابی امنیتی
- تصمیم‌گیری در رابطه با شکایات در زمینه نتیجه ارزیابی امنیتی و ارائه روالی برای شکایت یا فرجام خواهی
- جمع‌بندی نتایج ارزیابی‌ها و تصمیم گیری در خصوص صدور/عدم صدور گواهی محصولات
- تهیه و تدوین پروفایل حفاظتی با همکاری سازمان

مرکز افتا در تدوین و به روز رسانی پروفایل‌های حفاظتی محصولات، از مشاوره و همکاری تولیدکنندگان محصولات فناوری اطلاعات، محققان امنیتی، مصرف کنندگان محصول، کارشناسان سازمان و .... استفاده می‌کند. هدف اصلی از این مشاوره، همکاری در تولید پروفایل حفاظتی است که با مشارکت دولت، تولیدکنندگان و گروه‌هایی حاصل می‌گردد که نسبت به تهدیدات و آسیب‌پذیری‌های آن نوع از محصول آشنایی دارند.

در تدوین محتوای پروفایل حفاظتی موارد زیر لحاظ می‌شود:

- تهدیدات مربوط به محصول که موضوع پروفایل حفاظتی است بر اساس دانش عملی و تجربه فنی (تعریف مسائل امنیتی در پروفایل حفاظتی).
- حداقل کارکرد امنیتی برای کاهش تهدیدات معرفی شده (تعریف اهداف امنیتی).
- جمع آوری فعالیت‌های تضمین متناسب با محصول و هر الزام کارکردی در بند قبلی پوشش داده شود(تعریف الزامات امنیتی).

مرکز افتا نتایج ارزیابی‌های امنیتی را بررسی و در صورت تائید شدن، جهت صدور گواهی به سازمان معرفی می‌نماید. گواهی همراه با گزارش اعتبارسنجی و سند هدف امنیتی تائید می‌کند که محصول در یک آزمایشگاه معتبر با استفاده از «متدلوژی ارزیابی معیار مشترک» جهت بررسی انطباق آن با «استاندارد ارزیابی معیار مشترک» ارزیابی شده است. همچنین گواهی تائید می‌نماید که ارزیابی انجام شده بر اساس مفاد این سند (طرح ارزیابی امنیتی) انجام شده و نتایج ارزیابی آزمایشگاه با مدارکی که تولید کننده در طول ارزیابی ارائه نموده سازگار است.

۴,۲ سازمان

به عنوان یک نهاد دولتی همراه با مرکز افتا بالاترین سطح در استاندارد ارزیابی معیار مشترک است که درخواست ارزیابی محصول از سوی تولید کننده را دریافت و با هماهنگی مرکز افتا به آزمایشگاه ارجاع می‌دهد، همچنین منتشر کننده اسناد عمومی مرتبط با طرح ارزیابی امنیتی بوده و برای محصولی که توسط آزمایشگاه با موفقیت ارزیابی و توسط مرکز افتا تائید شده، گواهی صادر نموده و نام محصول گواهی شده همراه مستندات مربوط به آن را اطلاع رسانی می‌کند.

به طور کلی مسئولیت سازمان عبارت است از:

- اطلاع‌رسانی هرگونه تغییر در آزمایشگاه‌های مورد تائید مرکز افتا (همچون اضافه یا حذف آزمایشگاه‌ها از «طرح ارزیابی امنیتی») و هرگونه تغییر در حوزه اعتباربخشی آزمایشگاه‌ها
- دریافت شکایات و ارجاع به مرکز افتا در صورت نیاز
- صدور گواهی آزمایشگاه‌های تأیید شده توسط مرکز افتا به صورت مشترک با آن مرکز و انتشار آنها
- صدور گواهی محصولات پس از اعلام مرکز افتا و انتشار آن
- منتشر نمودن پروفایل‌های حفاظتی تائید شده توسط مرکز افتا

۵,۲ جایگاه مصرف کننده در طرح ارزیابی امنیتی

مهمترین هدف ارزیابی امنیتی محصولات، ورود محصولات ارزیابی شده و مطمئن به حوزه مصرف است. مصرف کننده باید صرفاً از محصولاتی استفاده نماید که مطابق این سند، گواهی امنیتی دریافت کرده باشند.

مصرف کننده در زمان بررسی محصولات و گواهی آن‌ها باید نکات زیر را در نظر داشته باشد:

- گواهی تنها برای نسخه‌ی خاصی از محصول و در سطح بکارگیری مشخصی صادر می‌شود.
- کیفیت مدارک ارزیابی و نتایج، تابعی از قابلیت شرح محصول توسط سند هدف امنیتی و همچنین الزامات تعیین شده در پروفایل حفاظتی، روش‌های بیان شده در متدلوژی ارزیابی معیار مشترک و روش‌های تست و ارزیابی محصول بیان شده در استاندارد معیار مشترک خواهد بود.
- نتایج ارزیابی امنیتی مربوط به محصولی است که در شرایط پیکربندی شده‌ای مورد ارزیابی قرار گرفته است. پیکربندی محصول بر روی عملکرد امنیتی آن اثر گذار است بنابراین مصرف کننده نسبت به عملکرد امنیتی محصول در پیکربندی که نموده مسئول است، زیرا ممکن است پیکربندی محصول توسط مصرف کننده متفاوت از آنچه که در محیط آزمایشگاه صورت گرفته باشد و در نتیجه عملکرد امنیتی محصول تحت تاثیر قرار گیرد و انتظار مصرف کننده را برآورده ننماید.

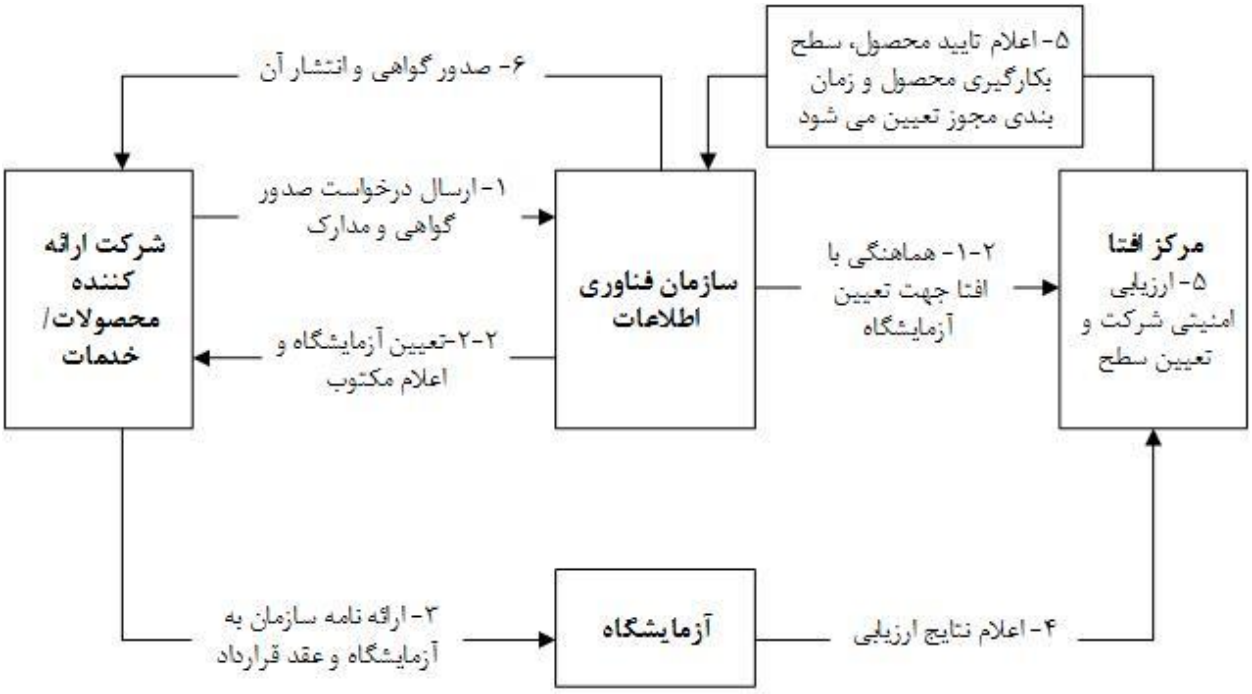
۳ ارزیابی امنیتی محصولات

در این بخش فرایند ارزیابی امنیتی محصولات و اقدامات ذی نفعان طرح ارزیابی امنیتی در طول مراحل مختلف ارزیابی محصول شرح داده می‌شود.

لازم به تاکید است که علاوه بر محصولات، پروفایل‌های حفاظتی نیز باید مورد ارزیابی قرار گیرند. جهت ارزیابی پروفایل حفاظتی لازم است نشان داده شود که این سند کامل بوده و محتوای قسمت‌های مختلف آن باهم سازگار است. ارزیابی پروفایل حفاظتی ممکن است به تنهایی انجام شود (براساس کلاس APE[۷] استاندارد ارزیابی معیار مشترک) یا ممکن است به عنوان بخشی از ارزیابی اولیه محصول در قبال پروفایل حفاظتی صورت گیرد. پروفایل حفاظتی ارزیابی شده و به تأیید رسیده توسط سازمان منتشر می‌شود.

همانگونه که در بخش آزمایشگاه‌ها شرح داده شد آزمایشگاه‌ها باید قادر به انجام ارزیابی بی‌طرفانه در رابطه با برآورده نمودن الزامات امنیتی توسط هدف ارزیابی باشند. این فرایند تائید می‌کند که ارزیابی مطابق آنچه که در طرح ارزیابی امنیتی ارائه شده، انجام می‌شود و نتایج آزمایشگاه با حقایق ارائه شده در سند «گزارش فنی ارزیابی» سازگار است.

در شکل شماره (۲) فرایند ارزیابی امنیتی محصولات نشان داده شده است.



شکل ۲- فرایند ارزیابی امنیتی محصولات فتا

مطابق شکل شماره (۲) فرایند کلی ارزیابی امنیتی محصولات به شرح ذیل می‌باشد:

[۷] Assurance Protection Profile Evaluation

۱- تهیه مقدمات ارزیابی و آماده سازی اسناد و مدارک مورد نیاز توسط تولید کننده و مراجعه به سازمان و ارائه درخواست ارزیابی امنیتی محصول
۲- ارجاع درخواست ارزیابی از طرف سازمان به مرکز افتا و تعیین آزمایشگاه با هماهنگی با آن مرکز، اعلام مکتوب به تولید کننده و ارسال رونوشت نامه مذکور به آزمایشگاه
۳- مراجعه تولید کننده به آزمایشگاه معرفی شده همراه با نامه معرفی سازمان و انعقاد قرارداد بین تولید کننده و آزمایشگاه
۴- انجام ارزیابی امنیتی محصول و اعلام نتایج به مرکز افتا
۵- ارزیابی امنیتی شرکت و تعیین سطح فعالیت آن توسط مرکز افتا
۶- اعلام تأیید/عدم تأیید محصول، سطح بکارگیری آن و مدت اعتبار مجوز توسط مرکز افتا بر اساس جمع‌بندی نهایی نتایج ارزیابی‌ها که توسط مرکز افتا انجام می‌شود.
۷- صدور گواهی توسط سازمان بر اساس بند ۶ (اعلام نظر مرکز افتا) و انتشار آن

فرایند فوق در چهار فاز اصلی انجام می‌شود که عبارتند از:
فاز اول: آماده سازی
درخواست تولید کننده
توافق اولیه بین آزمایشگاه و تولید کننده

فاز دوم: ارزیابی اسناد هدف امنیتی
بررسی و نهایی سازی سند هدف امنیتی

فاز سوم: ارزیابی فنی
ارزیابی روش تست محصول و روش تست آسیب‌پذیری

فاز چهارم: پایان ارزیابی محصول
صدور گواهی
نگهداری

۴ گواهی ارزیابی امنیتی محصول

همانگونه که در فرایند ارزیابی امنیتی محصولات (شکل شماره ۲) ذکر شد، مرکز افتا بر اساس بررسی ارزیابی‌ها، سطح بکارگیری محصول و مدت اعتبار را تعیین و جهت صدور گواهی به سازمان معرفی می‌نماید و در پایان

گواهی محصول توسط سازمان منتشر می شود. پیش از صدور گواهی لازم است تا تولید کننده نسبت به امضای تعهدنامه استفاده از گواهی اقدام نماید.

۱,۴ استفاده از گواهی استاندارد ارزیابی معیار مشترک

همانگونه که در بخش ۲-۵ سند (جایگاه مصرف کننده در طرح ارزیابی امنیتی) بیان شد، گواهی امنیتی محصول برای نسخه‌ی خاصی از محصول، با پیکربندی تعیین شده و در سطح بکارگیری مشخصی صادر شده است. مصرف کننده با رعایت ملاحظات ذکر شده بایستی اقدام به تهیه محصول دارای گواهی امنیتی نماید و تولید کننده می‌باید، محصول را مطابق گزارش اعتبارسنجی و گواهی منتشر شده، در سطح بکارگیری تعیین شده، به فروش برساند.

۲,۴ نگهداری گواهی محصول

روال‌های نگهداری از گواهی استاندارد معیار مشترک، توسط برنامه نگهداری که در سند «تداوم گواهی: راهنمایی برای نگهداری گواهی و ارزیابی مجدد» شرح داده شده، اعمال می‌گردد. در فرایند تداوم گواهی، تغییرات معنادار[۸] محصول در این بازه زمانی بررسی می‌شود، نتایج بررسی مشخص می‌کند که محصول به ارزیابی مجدد نیاز دارد یا خیر. تصمیم در رابطه با اینکه تغییر محصول معنادار بوده یا خیر، برعهده مرکز افتا می‌باشد. همچنین تولید کننده موظف است تا هر ساله گزارشی تحت عنوان «تحلیل آسیب پذیری» برای محصول دارای گواهی خود تهیه و به مرکز افتا ارسال نماید.

تولید کننده ممکن است پیش‌بینی ارزیابی مجدد محصول را نماید، بنابراین روال نگهداری گواهینامه را در مراحل ابتدایی شروع ارزیابی در نظر می‌گیرد تا فعالیت‌های آتی در این رابطه را به حداقل برساند.

برای اطلاع از جزئیات بیشتر در زمینه فرایند نگهداری گواهی به سند «تداوم گواهی: راهنمایی برای نگهداری و ارزیابی مجدد» مراجعه شود.

۵ نظارت

نظارت بر ارزیابی امنیتی محصولات در سه سطح انجام به شرح ذیل انجام می‌شود:

- نظارت بر اعتبار آزمایشگاه و رصد و پایش آن از جهت استمرار شرایطی که منجر به اعتبار بخشی آزمایشگاه و صدور گواهی فعالیت آن شده است.
- نظارت بر فرایند ارزیابی امنیتی محصولات و پایش عملکرد ذی نفعان
- نظارت بر محصول پس از بکارگیری در حوزه مصرف

[۸] تغییراتی که منجر به تغییر شرایط محصول با شرایط تست در آزمایشگاه گردیده است نظیر تغییر پیکربندی، قابلیت‌ها، اجزاء و غیره

۱,۵ نظارت بر اعتبار آزمایشگاه

همانگونه که پیشتر شرح داده شد، آزمایشگاه جهت فعالیت در حوزه ارزیابی امنیتی می‌باید دارای شرایطی باشد تا موفق به دریافت گواهی از مرکز افتا و سازمان گردد (جهت مشاهده شرایط اعتبار بخشی آزمایشگاه به سند <<راهنمای اعتباربخشی آزمایشگاه >> مراجعه شود). پس از دریافت گواهی فعالیت، مرکز افتا استمرار شرایط مذکور را در آزمایشگاه رصد می‌کند و در صورتیکه آزمایشگاه شرایط لازم که براساس آن اعتباربخشی شده است را از دست بدهد، اقدام مقتضی نظیر تذکر جهت رفع، عدم تمدید اعتبار، تعلیق اعتبار، لغو اعتبار و .... به عمل خواهد آورد.

۲,۵ نظارت بر فرایند ارزیابی محصول

این نظارت، نظارت بر فرایند ارزیابی امنیتی محصولات و پایش نحوه فعالیت ذی نفعان می‌باشد. پس از آنکه فرایند ارزیابی امنیتی محصول آغاز می‌شود، مرکز افتا بر فعالیت ذی نفعان نظیر تولید کننده و آزمایشگاه نظارت می‌کند. هدف از این نظارت آن است که اطمینان حاصل شود کلیه طرفهای درگیر در این فرایند، وظایف خود را به درستی انجام می‌دهند و به استانداردها، خط مشی‌ها، آیین نامه‌ها، مقررات، روالها و دستورالعمل‌های ابلاغی پایبند هستند. این نظارت در کل فرایند ارزیابی انجام می‌شود و بدیهی است که تأیید نتایج ارزیابی آزمایشگاه و مجوز صدور گواهی محصولات منوط به گزارش نظارت می‌باشد.

۳,۵ نظارت پس از اخذ گواهی

سومین سطح از نظارت، نظارت پس از ارزیابی امنیتی محصول و دریافت گواهی می‌باشد. این نظارت شامل دو بخش است:

- **نظارت بر محصول**

پس از آنکه محصول، فرایند ارزیابی امنیتی را به طور کامل طی کرده و موفق به دریافت گواهی گردید، در حوزه مصرف مورد استفاده قرار می‌گیرد. در این مرحله مرکز افتا بر محصول نظارت می‌کند و در صورت عدم تطابق محصول مورد استفاده با نمونه محصولی که در آزمایشگاه ارزیابی شده و یا کشف و بروز آسیب پذیری در محصول که نیاز به رفع و وصله نمودن داشته باشد و یا هر مورد دیگری، مرکز افتا موارد را به آزمایشگاه و تولید کننده جهت اقدامات مقتضی ارجاع داده و در صورت محرز شدن تخلف هریک، طبق ضوابط مقرره اقدام خواهد نمود.

- **نظارت بر مصرف کننده**

پس از آنکه محصول گواهی دریافت نمود، مرکز افتا علاوه بر نظارت بر آن در حوزه مصرف، بر مصرف کنندگان (در حیطه وظایف قانونی خویش) نظارت می‌کند تا اطمینان حاصل کند که آنها صرفاً از محصولاتی استفاده می‌کنند که گواهی امنیتی دریافت نموده‌اند.