جمهوری اسلامی ایران
ریاست جمهوری
مرکز مدیریت راهبردی افتا

معرفی خدمات افتا

اردیبهشت ۱۴۰۰


بسم الله الرحمن الرحيم

فهرست مطالب

مقدمه

با توجه به گستردگی خدمات در حوزه فناوری اطلاعات و امنیت فناوری اطلاعات و درهم تنیدگی‌های موجود که باعث ابهام در تمییز خدمات افتایی می‌شود، سند جاری با هدف معرفی خدماتی که در زمان تدوین این سند تحت پوشش گواهی‌های افتا می‌باشند تدوین شده است.

در این سند علاوه بر عنوان و تعریف خدمات افتا، اسناد تکمیلی تدوین شده برای گرایش‌های مختلف آدرس‌دهی شده است. این اسناد شامل اسناد معرفی، الزامات و دستورالعمل‌ها، راهنماهایی می‌باشد که لازم است در هر زمان با مراجعه به وب‌سایت افتا، آخرین نسخه منتشر شده از این اسناد مورد بهره‌برداری قرار بگیرد.

۱- خدمات مدیریتی افتا

منظور از خدمات مدیریتی افتا، خدماتی از جنس طراحی‌های کلان و ساختاری، طرح‌ریزی، برنامه‌ریزی، بهبود و ساماندهی، سنجش و پیشگیری مخاطرات امنیتی در سازمان‌ها و تدوین نظام‌ها و سیاست‌های امنیتی و ممیزی انطباق با استانداردهای موجود در این حوزه‌هاست.

در حال حاضر خدمات مدیریتی افتا شامل دو گرایش مشاوره استقرار استانداردهای امنیت اطلاعات و ارتباطات، و ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات است و تنها بر سیستم مدیریت امنیت اطلاعات (ISMS) متمرکز شده است.

۱-۱- مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات

در حالت کلی مشاوره استقرار سیستم مدیریت امنیت اطلاعات (ISMS)، سیستم مدیریت تداوم کسب و کار (BCM)، سیستم مدیریت بازیابی پس از فاجعه (DRM)، سیستم مدیریت مخاطرات (RM)، سیستم مدیریت رخداد (IM) و مانند آنها در حوزه تعریف این خدمت می‌گنجند.

اما در حال حاضر با توجه به اینکه دارندگان این پروانه صرفا از لحاظ توانمندی مشاوره استقرار سیستم مدیریت امنیت اطلاعات احراز صلاحیت شده‌اند، صدور پروانه تنها برای این استاندارد انجام می‌پذیرد. دارنده این پروانه موظف است در هریک از گام‌های پروژه استقرار سیستم مدیریت امنیت اطلاعات از ابتدا (تعیین دامنه) تا مراحل پایانی (آماده‌سازی برای ممیزی شخص ثالث/ آموزش و آگاهی‌رسانی) بر اساس سند «الزامات استقرار سیستم مدیریت امنیت اطلاعات» که در وبسایت مرکز افتا منتشر شده است، ایفای نقش نماید.

یادآور می‌شود که مسئولیت اصلی استقرار سیستم مدیریت امنیت اطلاعات در یک سازمان برعهده مدیریت ارشد آن سازمان کارفرما است و رعایت مفاد سند مذکور و نیز سند «راهنمای تعیین دامنه» می‌توانند در اجرای مسئولیت‌های کارفرما تاثیر بسزایی داشته باشد.

۲-۱-ممیزی انطباق استانداردهای امنیت اطلاعات و ارتباطات

این گرایش در حال حاضر متمرکز بر ممیزی انطباق با استاندارد ISO 27001 و در صورت احراز صلاحیت از نظر ممیز، توصیه ممیزی شونده به مرکز افتا برای دریافت گواهینامه ملی انطباق با این استاندارد می‌باشد.

شایان ذکر است که بر اساس گزارش ممیزی ارائه شده به کمیته تخصصی مرتبط در مرکز افتا، در خصوص وضعیت نهایی انطباق ممیزی شونده با ISMS تصمیم‌گیری می‌شود.

۲- خدمات فنی افتا

۲-۱-نصب و پشتیبانی امنیتی محصولات فتا

کاربرد این پروانه فعالیت تنها در قراردادهایی است که کارفرما با رعایت موارد بیان شده در این سند یک محصول فتایی را به همراه خدمات نصب و پشتیبانی آن خریداری می‌کند. به عبارت دیگر خدمات نصب و پشتیبانی محصولات فتا شامل فعالیت‌های زیر است:

- فروش، نصب و راه‌اندازی اولیه محصولات
- پشتیبانی و نگهداری محصولات شامل
  - پشتیبانی فنی، ضمانت، عیب‌یابی، رفع نقص‌ها و باگ فیکس، نگهداری زمانبندی شده (مدت دار مثلا ماهیانه)
  - انواع بروزرسانی‌ها اعم از بروزرسانی وصله‌ها، بروزرسانی محتوای امنیتی (محصولات امنیتی مانند آنتی‌ویروس) و بروزرسانی نسخه محصول
  - خدمات جایگزینی و تعمیر سخت‌افزار
  - آموزش استفاده و چگونگی راهبری محصول

لازم به ذکر است فعالیت‌های زیر در حوزه پوشش این پروانه نمی‌گنجند و شرکت‌های ارائه دهنده این خدمات لازم است برای پروانه امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها اقدام کنند:

- پشتیبانی و نگهداری شبکهOT/IT ،
- مشاوره و طراحی شبکه،
- طراحی و مشاوره امنیت شبکه،
- نصب، راه‌اندازی و پشتیبانی محصولات حوزه امنیت شبکه (از قبیل انواع فایروال/ فایروال نسل بعدی، سامانه‌های تشخیص و جلوگیری از نفوذ، سامانه‌های مدیریت یکپارچه تهدیدات، سامانه‌های مدیریت رخدادها و حوادث امنیتی)

درحال حاضر در وب‌سایت مرکز افتا اسناد مربوط به این گرایش به شرح ذیل منتشر شده است:

- حوزه صنعتی:
  - «دستورالعمل امنیت اطلاعات سیستم‌های مانیتورینگ ایستگاه‌های گاز»
  - «الزامات امنیتی عملیاتی زیرساخت‌های حیاتی صنعتی»
- محصولات نرم‌افزاری:
  - الزامات امنیتی ارائه محصولات نرم افزاری سازمانی به زیرساختهای حیاتی
  - الزامات امنیتی زیرساختهای حیاتی در استفاده از محصولات نرم افزاری سازمانی

دسته بندی تعیین شده محصولات برای این پروانه در حال حاضر به شرح ذیل است:

- سامانه‌های اسکادا
- سامانه‌های کنترل محلی و DCS
- زیرساخت‌های اندازه‌گیری پیشرفته
- محصولات حوزه امنیت صنعتی
- تجهیزات شبکه (از قبیل سوییچ، روتر، مودم)
- محصولات سرویس دهنده شبکه (از قبیل سرور پست الکترونیک)
- محصولات ضدبدافزار/ محافظت از نقطه نهایی
- محصولات مدیریت آسیب‌پذیری و وصله‌ها
- محصولات مدیریت دسترسی تحت شبکه (PAM, NAC, Remote Access)
- محصولات تامین امنیت داده (DLP, DRM)
- سرورها و تجهیزات ذخیره، بازیابی و پشتیبان‌گیری اطلاعات
- محصولات مجازی سازی
- تجهیزات رمزنگاری (VPN, Token, HSM)
- محصولات ارائه خدمات مبتنی بر محتوی (DMS, CMS, BPMS, ERP, CRM)
- ابزارهای پایش شبکه
- تجهیزات مخابراتی
- محصولات پایش تصویر
- محصولات حوزه سلامت
- انتقال صدا و تصویر در بستر شبکه(VOIP)
- حوزه پخش فراورده‌های نفتی
- سامانه‌های نرم‌افزاری (سامانه‌های نرم‌افزاری بومی دارای گواهی ارزیابی امنیتی محصولات افتا)

۳- خدمات آموزشی افتا

این حوزه خدمات شامل ارائه آموزش کلیه دوره‌های امنیتی در سطوح و موضوعات مختلف به متقاضیان است. دامنه این حوزه مربوط به آموزش‌هایی می‌باشد که منجر به دریافت گواهینامه‌های ملی و بین‌المللی در زمینه دوره‌های آموزشی امنیت اطلاعات و ارتباطات گردد.

درحال حاضر مشخصات دوره‌های آموزشی مورد تایید افتا در قالب سند «معرفی دوره‌های آموزشی افتا» در وب‌سایت مرکز افتا منتشر شده است.

۴- خدمات عملیاتی افتا

خدمات عملیاتی افتا، بیشتر بر مهارت‌های خاص و فنی کارشناسان برای پیاده‌سازی و یا حصول اطمینان از عملکرد مناسب کنترل‌های پیاده‌سازی شده تاکید دارد. در واقع تمرکز اصلی این گرایش اقدامات عملیاتی امنیتی است که توسط کارشناسان این حوزه برای پایش، ارزیابی و ارتقاء سطح امنیت انجام می‌پذیرد و معمولا برخلاف گرایش نصب و پشتیبانی، مبتنی بر محصول/گروه محصول خاصی نیست.

۴-۱- آزمون و ارزیابی امنیتی

خدمت آزمون و ارزیابی امنیتی شامل کلیه خدمات ارزیابی امنیتی نرم‌افزار، تجهیزات، سرویس‌ها و سامانه‌ها، آزمون نفوذپذیری و آزمون آسیب‌پذیری می‌باشد. در واقع اگر نیاز به یکی از فعالیت‌های زیر باشد، این پروانه می‌بایست مورد استفاده قرار بگیرد:

- پویش آسیب‌پذیری سامانه‌ها و شبکه IT/OT
- ارزیابی آسیب‌پذیری سامانه، تجهیزات و سرویس ها
- آزمون نفوذپذیری سامانه، تجهیزات و سرویس ها
- ارزیابی امنیتی سامانه، تجهیزات و سرویس ها

درحال حاضر سند «الزامات دارندگان پروانه فعالیت خدمت آزمون و ارزیابی در اجرای پروژه‌های آزمون نفوذپذیری» در وب‌سایت مرکز افتا منتشر شده است.

۴-۲- کشف نقص امنیتی

کشف نقص امنیتی خدمتی است که در آن سامانه/سامانه‌های کارفرما توسط هکرها 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 دو صورت زیر قابل انجام است:

- باگ بانتی عمومی : 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 : 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 در روی شبکه محلی قرار دارد و یا از طریق VPN قابل دسترس است). همچنین در شرایط خاص ممکن است مشتری درخواست کند که برای سامانه ای که در دسترس عموم قرار دارد، تست نفوذ از مسیر مشخصی تحت مالکیت شرکت برگزار کننده مسابقه انجام پذیرد.

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، نقص های کشف شده توسط شرکت کنندگان در مسابقه را ارزیابی و در صورت صحت به اطلاع مشتری می‌رساند تا اقدامات لازم برای رفع ان صورت پذیرد. همچنین بر اساس سطح نقص گزارش شده، جوایزی از طرف مشتری به کشف کننده نقص مذکور تعلق می‌گیرد.

درحال حاضر اطلاعات این گرایش در قالب سند «معرفی خدمت مسابقات کشف نقص امنیتی» در وب‌سایت مرکز افتا منتشر شده است.

۴-۳- پیاده‌سازی مرکز عملیات امنیت

خدمات مرتبط با پیاده‌سازی مرکز عملیات امنیت به خدماتی اطلاق می‌شود که وظیفه راه‌اندازی و پشتیبانی از تجهیزات و سامانه‌های مرتبط با مرکز عملیات امنیت را برعهده دارد و برای طراحی ساختار، ارائه راهکارهای مقابله با حوادث امنیتی، تدوین فرایندهای مرتبط، استقرار استانداردهای مرتبط و آموزش کاربران مرکز عملیات امنیت در محیط کارفرما مورد استفاده قرار می‌گیرد. در واقع پیاده‌سازی مرکز عملیات امنیت شامل سه بعد فرآیندها (رویه‌ها)، تجهیزات و آموزش نیروی انسانی می‌باشد.

۴-۴- راهبری مرکز عملیات امنیت

خدمات مرتبط با راهبری مرکز عملیات امنیت به خدماتی اطلاق می‌شود که به منظور راهبری سامانه‌های مرکز عملیات امنیت، پایش و تحلیل رخدادهای امنیتی، تهیه و تدوین گزارش‌های رخدادهای امنیتی، در محیط کارفرما، مورد استفاده قرار می‌گیرد.

۴-۵- پاسخ به رخدادهای سایبری

خدمات مرتبط با پاسخ به رخدادهای سایبری به خدماتی اطلاق می‌شود که به منظور شناسایی حوادث امنیتی و سایبری رسیدگی به موقع به آنها مورد استفاده قرار می‌گیرد.

۴-۶- امن‌سازی و مقاوم‌سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها

این خدمت به فعالیت‌هایی در خصوص امن‌سازی و مقاوم‌سازی شبکه، سامانه‌ها، سرویس‌ها و تجهیزات نرم‌افزاری و سخت‌افزاری می‌پردازد. این گرایش شامل پنج زیر گرایش زیر می‌باشد:

- پیکربندی امن: این زیر گرایش شامل فعالیت‌ها در حوزه نصب و پشتیبانی محصولات امنیت شبکه می‌باشد. با توجه به آنکه نصب و پشتیبانی محصولات امنیت شبکه نیاز به دانش امنیتی و امن‌سازی (علاوه بر دانش تخصصی محصولات قابل پشتیبانی) دارد، نصب و پشتیبانی این نوع از محصولات نیاز به این گواهی دارد.
- امن‌سازی شبکه‌های فناوری اطلاعات (IT): ارائه دهنده این زیر گرایش، نسبت به امن‌سازی و مقاوم‌سازی شبکه، سامانه، سرویس، تجهیزات نرم‌افزاری و سخت‌افزاری برای مقابله با بدافزارها و دسترسی‌های غیرمجاز، در محیط کارفرما اقدام می‌نماید.
- پیکربندی امن محصولات صنعتی: این حوزه دربردارنده فعالیت‌هایی در خصوص نصب سامانه‌های امنیتی در حوزه زیرساخت‌های صنعتی نظیر دیتا دیود صنعتی، پایشگر شبکه صنعتی، انواع لاگر، فایروال صنعتی، نرم افزار Whitelist، مدیریت یکپارچه به روزرسانی در سطح فیلد و .... می‌باشد.
- مشاوره امن سازی و مقاوم‌سازی زیرساخت صنعتی: این حوزه دربردارنده فعالیت‌هایی در خصوص وضعیت امنیت سایبری زیرساخت صنعتی را به صورت غیرفعال[1] ارزیابی و برای ارتقا آن راه حل ارائه

[1] Passive

دهند. دارندگان این نوع پروانه اجازه انجام عملیات فعال و ایجاد تغییراتی نظیر نصب نرم افزار، افزودن تجهیز جدید و ... در زیرساخت صنعتی را ندارند.

- امن‌سازی شبکه‌های صنعتی: در این زیرگرایش، شرکت ارائه دهنده خدمت اقدام به امن‌سازی و مقاوم‌سازی سامانه‌های کنترل صنعتی برای مقابله با بدافزارها و دسترسی‌های غیرمجاز، در محیط کارفرما می‌نماید. این سامانه‌ها شامل کلیه نرم افزارها، سخت افزارها و سایر عوامل مرتبطی هستند که به منظور اندازه‌گیری الکترونیکی، کنترل، مانیتورینگ، عیب‌یابی و ایمنی فرآیندهای صنعتی تولیدی، انتقالی و توزیعی به کار گرفته می‌شوند.

۷-۴- پیاده‌سازی امنیت فیزیکی و محیط پیرامونی

این گرایش شامل طراحی، نصب، پیکربندی و پشیبانی از راه‌حل‌های ایجاد امنیت فیزیکی و محیط پیرامونی است. پروژه‌هایی با ماهیت طراحی و پیاده‌سازی راهکارهای امنیت محیط پیرامونی از جمله وارد ذیل در دامنه این پروانه قرار می‌گیرد:

- امن‌سازی و مقاوم‌سازی اتاق سرور و مراکز داده
- طراحی و پیاده‌سازی سامانه‌های اطفای حریق در محیط‌های مرتبط با فناوری اطلاعات
- طراحی و پیاده‌سازی راه‌حل‌های تامین مطمئن انرژی برای تجهیزات فناوری اطلاعات
- طراحی و پیاده‌سازی سامانه‌های کنترل دسترسی فیزیکی مانند سیستم‌های کنترل ورود/خروج