ارائه نیازهای فناورانه حوزه امنیت فناوری اطلاعات (افتا)

حوزه امنیت اطلاعات و ارتباطات

عنوان نیاز فناورانه

سامانه ضدبدافزار بومی

شرح نیاز فناورانه

یکی از موضوعاتی که به منظور افزایش وارتقاء سطح امنیت سیستم های رایانه ای بکارگیری می گردد ، نرم افزارهای ضدبدافزار می باشند.امروزه بدافزارهای رایانه ای یکی از تهدیدات اصلی در حوزه فناوری اطلاعات می باشد و تکیه بر ابزارهای غیر بومی و وابستگی به ابزارهای خارجی دراین حوزه می تواند چالش ها و خطرات جدی را در مواقع بحرانی و حساس ایجاد نماید. لذا تولید ضدبدافزار بومی در این راستا ، منجر به تقویت توان دفاعی در حوزه امنیت فاوا خواهد شد.

حوزه فناوری تقاضا

امنیت اطلاعات و ارتباطات

حوزه صنعتی تقاضا

امنیت انتظامی درفضای سایبری

پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

قابلیت تشخیص و شناسایی بدافزارها از طریق روشهای Signature Based و Heuristic با درصدشناسایی قابل رقابت با سایرضدبدافزارهای مطرح غیربومی و بومی

قابلیت تنظیم اسکن زمانبندی شده جهت اجرای خودکار در فواصل زمانی مشخص

امکان نصب و راه اندازی سرورهای ضدبدافزاربصورت سلسله مراتبی با ساختار Master-Slave

پایین بودن درصدشناسایی غلط (False Positive)

فناوری‌ها و راه‌حل‌های نامطلوب

مدل همکاری مطلوب

مدل تعامل و مشارکت پژوهشی و فناوری

ارائه نیازهای فناورانه حوزه امنیت فناوری اطلاعات (افتا)

حوزه امنیت اطلاعات و ارتباطات

عنوان نیاز فناورانه

- طرح احراز هویت غیرحضوری متقاضیان خدمات الکترونیک بر مبنای سنجه‌های بیومتریکی
- طرح ارتقاء امنیت پایگاه‌های داده (رمزنگاری، علامت‌گذاری و امضای دیجیتال داده‌ها)
- ارزیابی تاب آوری سایبری سامانه‌ها و زیرساخت‌های ارتباطی

شرح نیاز فناورانه

- طرح احراز هویت غیرحضوری متقاضیان خدمات الکترونیک بر مبنای سنجه‌های بیومتریکی

فراهم شدن بستری برای توسعه و تسهیل خدمات دولت الکترونیک برای شهروندان از دغدغه های اصلی سازمان است. با توجه به شرایط مختلف گرایش عمومی به عدم مراجعه حضوری و انجام کارها از راه دور روز به روز بیشتر می‌شود. اعلیرغم تغییرات گسترده در حوزه فناوری اطلاعات و ارتباطات، بسیاری از این خدمات همچنان به روش سنتی و حضوری ارائه می‌شوند. لذا به نظر می‌رسد که در این رویکرد باید بازنگری شده و خدمات از درگاه‌هایی مثل دفاتر خدمات الکترونیک سازمانی، به منازل و محل کار مردم برده شوند و ساعات ارائه خدمات نیز ۷*۲۴ شود. این موضوع مستلزم توسعه سامانه‌های و زیرساخت‌های موجود و یا ایجاد موارد جدیدی از آنها است. اما این تنها چالشی نیست که فراروی تحقق این رویکرد قرار دارد. چالش مهم‌تر در حوزه امنیت این خدمات مطرح می‌باشد و آن چالش چیزی نیست جز احراز هویت فرد متقاضی خدمات، به گونه‌ای که سازمان مطمئن شود خدمت به هویت واقعی که ادعا شده ارائه می‌شود و امکان سوء استفاده از این خدمات برای دیگران هم وجود ندارد.

شرح نیاز فناورانه

- طرح ارتقاء امنیت پایگاه‌های داده (رمزنگاری، علامت‌گذاری و امضای دیجیتال داده‌ها)

ارتقاءِ امنیت پایگاه داده، یک گزاره نسبی بوده که درک صحیح از آن مستلزم ارائه یک تعریف دقیق‌تر از مطلوبات و انتظاراتی است که در مقوله ارتقاءِ امنیت دنبال می‌شوند. آنچه در این طرح از ارتقاءِ امنیت پایگاه داده انتظار می‌رود که محقق شود، عبارتست از:

- جلوگیری از تغییر غیرمجاز محتوای پایگاه داده
  - در سطح رکورد
  - در کل پایگاه داده
- امکان تشخیص هویت اعمال کننده تغییرات مجاز و عدم انکار
- امکان تعیین زمان اعمال تغییرات (مجاز/غیرمجاز)
- امکان بازیابی اطلاعات بر اساس زمان اعمال تغییرات غیرمجاز از پایگاه داده پشتیبان
- ایجاد محرمانگی برای جلوگیری از نشت اطلاعات انبوه
- جلوگیری از نشت اطلاعات در صورت بروز حملات در سطح برنامه‌های کاربردی بهره‌بردار از پایگاه داده بر اساس احراز هویت آنها در چرخه دسترسی به اطلاعات
- امکان نظارت بر عملکرد مدیران (Administrators) پایگاه داده

حوزه فناوری تقاضا

امنیت اطلاعات و ارتباطات

حوزه صنعتی تقاضا

امنیت فضای سایبری

پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

طرح احراز هویت غیرحضوری متقاضیان خدمات الکترونیک بر مبنای سنجه‌های بیومتریکی

- دستورالعملها و الزامات قانونی و فنی کشوری رعایت گردند.
- خدمات موجود بسته به سطح حساسیت، بر اساس روش‌های مختلف احراز هویت و یا ترکیبی از آنها، به صورت غیرحضوری قابل ارائه باشند.
- خدماتی که در حال حاضر ارائه نمی‌شوند یا قابل ارائه نیستند، با ایجاد بستر لازم در قالب این طرح، از این پس قابل ارائه شوند.
- امنیت در فرایند احراز هویت و ارائه خدمات ایجاد گردد و کسی به جای دیگری نتواند خدمات را دریافت نماید.
- اقدامات انجام شده در راستای دریافت یک خدمت قابل انکار نباشد.

پارامترهای عملکردی لازم (الزامات راه‌حل‌های

طرح ارتقاء امنیت پایگاه‌های داده (رمزنگاری، علامت‌گذاری و امضای دیجیتال داده‌ها)

- دستورالعملها و الزامات قانونی و فنی کشوری و لشکری رعایت گردند.
- اعمال امضای دیجتال بر روی فیلدها/رکوردها و محتوای پایگاه داده
- رمزنگاری فیلدها/رکوردها و محتوای پایگاه داده
- اعمال مهر زمانی بر روی امضای دیجیتال اطلاعات
- ست کردن تریگرهای مختلف حساس به واکشی بیش از حد اطلاعات بویژه وقتی از یک آدرس واحد انجام می‌شود.
- اعمال رمزنگاری و امضای دیجیتال بر روی تمامی لاگ‌ها
- استفاده از هانی‌پات برای گرفتار کردن مهاجم قبل از دسترسی به پایگاه داده اصلی
- استفاده از دیواره آتش ویژه برای پایگاه داده
- استفاده از سخت‌افزارهای امنیتی برای مدیریت کلیدهای رمز
- علامت‌گذاری داده‌ها با روش‌هایی نظیر پنهان‌نگاری
- تقویت مکانیزم‌های امنیت فیزیکی و کنترل دسترسی موجود

فناوری‌ها و راه‌حل‌های نامطلوب

- استفاده از روشهای سنتی و حضوری
- استفاده از فناوری هایی نظیر گذرواژه

مدل همکاری مطلوب

مدل تعامل و مشارکت پژوهشی و فناوری

ارائه نیازهای فناورانه حوزه امنیت فناوری اطلاعات (افتا)

حوزه امنیت اطلاعات و ارتباطات

عنوان نیاز فناورانه

- طرح احراز هویت غیرحضوری متقاضیان خدمات الکترونیک بر مبنای سنجه‌های بیومتریکی
- طرح ارتقاء امنیت پایگاه‌های داده ناجا (رمزنگاری، علامت‌گذاری و امضای دیجیتال داده‌ها)
- ارزیابی تاب آوری سایبری سامانه‌ها و زیرساخت‌های ارتباطی فاوا

شرح نیاز فناورانه

- ارزیابی تاب آوری سایبری سامانه‌ها و زیرساخت‌های ارتباطی فاوا

با توجه به اهمیت موضوع تاب آوری، شاخص ها و مدلهای متفاوتی در خصوص سنجش تاب آوری در حوزه های مدیریت سوانح اجتماعی، زنجیره تامین، تاب آوری سازمانی و .... ارائه شده است که غالبا دارای رویکردهای مفهومی بوده و قابل بهره برداری در خصوص موضوعات دیگر نظیر آمادگی سایبری نیستند.

حوزه فناوری تقاضا

امنیت اطلاعات و ارتباطات

حوزه صنعتی تقاضا

امنیت فضای سایبری

پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

- دستورالعملها و الزامات قانونی و فنی کشوری و لشکری رعایت گردند.
- اعمال مدل ها و چارچوب های متناسب با تاب آوری و بلوغ امنیت
- لحاظ نمودن مدل ارزیابی تاب آوری سایبری در زیرساخت‌های اختصاصی و مشترک
- استخراج مولفه ها مدل ارزیابی تاب آوری سایبری
- استخراج شاخص های مدل ارزیابی تاب آوری سایبری

فناوری‌ها و راه‌حل‌های نامطلوب

- استفاده از چک لیست های امنیتی

مدل همکاری مطلوب

مدل تعامل و مشارکت پژوهشی و فناوری