ارائه نیازهای فناورانه حوزه امنیت فناوری اطلاعات (افتا)

سازمان صدا و سیمای جمهوری اسلامی ایران

عنوان نیاز فناورانه

ردیف	عنوان
۱	سامانه پیشگیری از نشت اطلاعات در لایه میزبان و شبکه (DLP)
۲	سامانه پیشگیری از نشت اطلاعات در لایه داده (DLP)
۳	سامانه آگاهی وضعیتی سایبری (CSA)
۴	سامانه مدیریت حقوق دیجیتالی صوت و تصویر (DRM)
۵	سامانه مقابله با تهدیدات مقاوم پیشرفته (APT)
۶	سامانه تشخیص رسانه (فیلم و تصویر) جعلی (Deep Fake)
۷	سامانه مقابله با سواستفاده و سرقت محتوای رسانه ای (Piracy)
۸	سامانه تشخیص و مدیریت داده های تاریک (Dark Web)
۹	سامانه امن پشتیبان گیری و بازیابی داده ها
۱۰	تکمیل و توسعه گروه واکنش سریع به رخدادهای

شرح نیاز فناورانه

عنوان	سامانه پیشگیری از نشت اطلاعات در لایه میزبان و شبکه (DLP)
شرح	جلوگیری از نشت اطلاعات دربرگیرنده‌ی عوامل انسانی، فرایندها و سیستم‌هایی است که بر داده‌های در حال استفاده (سمت میزبان)، داده‌های در حال انتقال (در شبکه) و داده‌های ذخیره شده (در پایگاه‌های ذخیره‌سازی داده) نظارت دارند؛ بنابراین میزبان، شبکه و پایگاه ذخیره‌سازی، سه جایگاهی است که جلوگیری از نشت اطلاعات در آن صورت می‌پذیرد. سامانه پیشگیری از نشت اطلاعات در لایه میزبان و شبکه (DLP)، به محافظت از اطلاعات در حال تبادل در شبکه می‌پردازد و حاوی راهکاری جامع در جهت کاهش هرچه بیشتر خطر نشت و خروج عمدی و یا سهوی اطلاعات حساس سازمانی از طریق ارسال یا به‌اشتراک‌گذاری غیرمجاز آن‌ها در شبکه داخلی یا اینترنت از طریق ایمیل، چت، نرم‌افزارهای تحت وب و ... است. از این محصول می‌توان به‌عنوان ابزاری جهت افزایش بهره‌وری و کنترل کارایی کارکنان نیز بهره برد. مولفه‌های اصلی این پروژه عبارتند از: ❖ ماژول مانیتورینگ ❖ ماژول پیشگیری از تخلف ❖ ماژول حفاظت از ایمیل ❖ ماژول مدیریت مرکزی

شرح نیاز فناورانه

عنوان	سامانه پیشگیری از نشت اطلاعات در لایه داده (DLP)
شرح	جلوگیری از نشت اطلاعات دربرگیرنده‌ی عوامل انسانی، فرایندها و سیستم هایی است که بر داده‌های در حال استفاده (سمت میزبان)، داده‌های در حال انتقال (در شبکه) و داده‌های ذخیره شده (در پایگاه‌های ذخیره‌سازی داده) نظارت دارند؛ بنابراین میزبان، شبکه و پایگاه ذخیره‌سازی، سه جایگاهی است که جلوگیری از نشت اطلاعات در آن صورت می‌پذیرد. سامانه پیشگیری از نشت اطلاعات در لایه داده (DLP)، به محافظت از اطلاعات در حال تبادل در شبکه می‌پردازد و حاوی راهکاری جامع در جهت کاهش هرچه بیشتر خطر نشت و خروج عمدی و یا سهوی اطلاعات حساس سازمانی از طریق ارسال یا به اشتراکگذاری غیرمجاز آن‌ها در شبکه داخلی یا اینترنت از طریق ایمیل، چت، نرم افزارهای تحت وب و ... است. سامانه پیشگیری از نشت اطلاعات در لایه داده (DLP)

شرح نیاز فناورانه

عنوان	سامانه آگاهی وضعیتی سایبری (CSA)
شرح	با وجود پیشرفت‌های چشم‌گیر درزمینه‌ی تشخیص و شناسایی حملات سایبری، هنوز هم بسیاری از متخصصان حوزه امنیت سایبری بر این باورند که سامانه‌های تشخیص و شناسایی بلادرنگ ازلحاظ فنی برای آشکارسازی حملات سایبری پیچیده به اندازه کافی پیشرفت مطلوبی نداشته‌اند. در طرح طراحی اگاهی وضعیت سایبری، با ادغام داده‌ها و اطلاعات حاصل از عامل‌های توزیع‌شده ناهمگن در سامانه‌های تشخیص و شناسایی حملات سایبری، امکان توسعه سامانه تشخیص و شناسایی حملات سایبری با قابلیت اطمینان بالا برای شناسایی، ردگیری و ارزیابی وضعیت فضای سایبری که تحت تأثیر تهدیدات پیچیده متعدد هستند فراهم می‌شود. ایجاد آگاهی وضعیتی فضای سایبری در سامانه‌های تشخیص و شناسایی حملات سایبری این طرح با بهره‌گیری از فناوری ادغام داده‌های چند حسگری چارچوب مناسبی برای عملکرد آن ایجاد می کند. مهم‌ترین اهداف حاصل از اجرای این طرح عبارتند از: ❖ توانایی پیش بینی الگوهای خاص هر حمله و آسیب‌پذیری‌های شبکه و ساماانه‌ها در سیستم که برای حمله‌کنندگان بسیار مهم است و قابلیت تحلیل و بررسی آن‌ها ❖ توانایی شناسایی تهدیداتی که به‌مثابه بردار حمله بوده یا الگوهایی که پتانسیل یک حمله ضربه‌ای را دارند ❖ قابلیت ردگیری حملات سایبری چندمرحله‌ای و هماهنگ کردن اقدامات مرتبط با آن‌ها و ارائه

شرح نیاز فناورانه

عنوان	سامانه مدیریت حقوق دیجیتالی صوت و تصویر (DRM)
شرح	سیستم‌های مدیریت و حفاظت از حقوق مالکیت اطلاعات یا به اختصار (DRM) زمینه ای را برای مالکان آثار دیجیتال به‌گونه‌ای فراهم می‌کنند که هم برای خالق اثر و هم برای جامعه سودمند باشند. از یک سو، جامعه از فعالیت تولیدی پدیدآورندگان بهره‌مند می‌شود و از سوی دیگر، با اعطای حق مالکیت انحصاری آثار به پدید آورندگان آن‌ها و تأمین زمینه استیفای این حق، خلاقیت و تولید فرهنگی تقویت می‌شود بدین ترتیب پدیدآورندگان می‌توانند هزینه‌های خلق و تولید آثارشان را به‌گونه‌ای که مقبول جامعه است تأمین کنند. مهم‌ترین مواردی که در طراحی و به‌کارگیری سیستم مدیریت حقوق دیجیتالی (DRM) باید مدنظر قرار گیرند عبارتند از: ❖ نظارت وکنترل بر نحوه کاربرد، انتشار و استفاده از اطلاعات ❖ تضمین مالکیت اطلاعات پس از واگذاری ❖ جلوگیری از سرقت‌های داخل سازمانی ❖ مصونیت در مقابل نفوذهای اینترنتی ❖ نیاز به ایجاد تغییر در نرم‌افزارهای موجود ❖ نیاز به ارتباط دائم کاربر با سرورهای امن ❖ عدم امکان ویرایش داده‌های محافظت شده توسط کاربر ❖ عدم پشتیبانی از مالکیت‌های چندگانه

شرح نیاز فناورانه

عنوان	سامانه مقابله با تهدیدات مقاوم پیشرفته (APT)
شرح	تهدیدات مقاوم پیشرفته معمولاً از تکنیک‌های متنوع و گوناگونی از قبیل دانلودهای ناخواسته، تزریق SQL، بدافزار، نرم‌افزارهای جاسوسی، فیشینگ و هرزنامه‌ها استفاده می‌کنند. اغلب سامانه‌های دفاعی کنونی «نقطه‌محور» هستند و تنها از خود دفاع می‌کنند. این در حالی است که در رویکرد پدافند پویا، روش‌های مورداستفاده هم کلی‌نگر است، به این معنی که تمام مجموعه از حمله شرکای تجاری و تأمین‌کنندگان مواد اولیه را مدنظر داشته و پویا بوده و دقیقاً هم‌پای تهدیدات، روندی تکاملی دارند. اغلب روش‌های پدافندی چندلایه ایستا که توسط بسیاری از شرکت‌ها و با استفاده از برنامه‌های مختلف به کار گرفته شده‌اند، نمی‌توانند در برابر روش‌های مبتنی بر مهندسی اجتماعی نظیر «فیشینگ هدف‌اند» و «حملات روز صفر» مؤثر باشند. یک ساختار امنیتی چندلایه معمولی که لایه‌های آن از روش‌های متداول انطباق الگو یا امضای دیجیتال استفاده می‌کنند، نظیر سامانه‌های شناسایی و ممانعت، فایروال‌ها و دروازه‌های دیجیتال، تنها به ایجاد یک حس غلط امنیت، منجر می‌شوند. در طرح مقابله با تهدیدات مقاوم پیشرفته (APT)، راهکارهای هوشمند سازی پیرامون تهدیدات (TI) و راهکار شکارتهدیدات (TH) می‌بایست در کنار هم مورد بهره‌برداری قرار بگیرند تا نتیجه‌ی مطلوب حاصل شود. راهکارهای هوشمندی پیرامون تهدیدات و شکار تهدیدات دو راهکار مکمل و متمم می‌باشند که هر دو می‌توانند برای بالغ سازی و بهبود خروجی‌های حاصل از یکدیگر مؤثر باشند. شکار تهدیدات می‌بایست به‌عنوان راهکاری پویا جهت واکنش به هشدارها و تهدیدات احتمالی مورداستفاده واقع شود و منجر به شناخت روش‌ها و راهکارهای ممکن جهت افزایش وضوح دید هوشمندی پیرامون تهدیدات و قابلیت‌ها و امکانات قابل ارائه

شرح نیاز فناورانه

عنوان	سامانه تشخیص رسانه (فیلم و تصویر) جعلی (Deep Fake)
شرح	دیپ‌فیک نام یک تکنیک نرم‌افزاری مبتنی‌بر هوش‌مصنوعی است که در محتوای صوتی و تصویری دست می‌برد و آن را به‌دلخواه دگرگون می‌سازد؛ بنابراین نتیجه نهایی که به‌دست می‌آید، چیزی کاملاً متفاوت از حقیقت خواهد بود. درواقع نام این تکنیک نیز به‌درستی عملکرد آن را آشکار می‌سازد؛ دیپ‌فیک، ترکیبی از یادگیری عمیق (Deep Learning) و جعل (Fake) است. عدم امکان تشخیص جعلی یا واقعی بودن ویدئوها از سوی مخاطبان یا ذینفعان یک سازمان، می‌تواند گاه به آسیب‌های جبران ناپذیری منجر شود که این آسیبها می‌توانند دامنه ای وسیع از عدم اعتماد به سازمان تا صدماتی در ابعاد امنیتی، اقتصادی، سیاسی، اجتماعی و... و حتی سلامتی روحی و جسمی را شامل شوند. در طرح سامانه تشخیص رسانه (فیلم و تصویر) جعلی، مهم‌ترین اقدامات مدنظر عبارتند از: ❖ ارتقای سوادهای نوینی همچون سواد رسانه‌ای، خبری و بصری در فعالان حوزه روابط عمومی ❖ آموزش به دیگران در خصوص ارتقاء توان تشخیص اخبار و تصاویر جعلی و غیرجعلی ❖ استفاده از فناوری‌های رسانه‌ای از قبیل بهره‌گیری از جستجوی معکوس، توجه دقیق به‌جزئیات، توجه به متن، زیرمتن و فرامتن، استفاده از نرم‌افزارهای کنترل اصالت عکس و... ❖ بهره‌مندی از ابزارهای و امکانات روز رصد، نظارت و تحلیل اخبار، اطلاعات و داده‌ها ❖ بهره‌مندی از آرشیوی غنی از محتواهای به‌روز سازمانی در حوزه‌های مختلف ❖ برنامه‌ریزی صحیح در روند خبررسانی، آگاهی بخشی و اطلاع‌رسانی به موقع و مناسب و حذف موانع بازدارنده در جریان اطلاع‌رسانی

شرح نیاز فناورانه

عنوان	سامانه مقابله با سواستفاده و سرقت محتوای رسانه ای (Piracy)
شرح	کپی غیرقانونی محتوای تولید شده خصوصا محتوای متنی یکی از مهم‌ترین دغدغه‌های مدیران سایت‌های محتوا محور و بلاگ‌ها است. محتوای غیر متنی مانند تصاویر، ویدئو و اسلاید به‌راحتی قابل شناسه‌گذاری است و معمولاً کمتر از متن مورد سوءاستفاده قرار می‌گیرد. «تغییر رسانه» و «تغییر فرمت» محتوا شیوه‌های متداولی است که دستاورد آن گردش یکسان اطلاعات بین رسانه‌های اجتماعی و سایت‌هاست، در نهایت تولید کننده متضرر می‌شود چراکه مخاطب نمی‌داند چه کسی تولید کننده اول است و به چه دلیل آن را تولید کرده است. مهم‌ترین اقداماتی که در طرح سامانه مقابله با سواستفاده و سرقت محتوای رسانه‌ای (Piracy) مدنظر است عبارتند از: ❖ استفاده از فرایندها و تکنیک‌های مناسب جهت جلوگیری از کپی برداری و انتشار خودکار محتوا ❖ استفاده از ابزارهای فنی نظیر ابزار وب‌مستر گوگل برای جلوگیری از ایندکس شدن محتوا ❖ تولید محتوا در یک ساختار منحصر به‌فرد پیوسته، منظم، هدفمند ❖ ارائه آموزش‌های لازم از قبیل اطلاع‌رسانی محتوای خود بعد از انتشار از طریق شبکه‌های اجتماعی جهت جلوگیری یا کاهش سوءاستفاده یا سرقت محتوای رسانه‌ای تولید شده ❖ استفاده از مکانیسم‌های اعلام اصالت نظیر مکانیسم اعلام اصالت مطلب گوگل یا Google Authorship

شرح نیاز فناورانه

عنوان	سامانه تشخیص و مدیریت داده های تاریک (Dark Web)
شرح	اطلاعاتی که یک سازمان در طول فعالیت عادی خود، گردآوری، پردازش و ذخیره‌سازی کرده است و جزیی از دارایی‌های آن به‌حساب می‌آید؛ اما نتوانسته است برای مقاصد دیگری از آن‌ها استفاده کند جزو داده‌های تاریک محسوب می‌شوند. اغلب داده‌های سازمان‌های بزرگ را باید در شمول داده‌های تاریک تلقی کرد. در طرح سامانه تشخیص و مدیریت داده‌های تاریک، ابتدا باید داده‌های تاریک معاونت تعریف شناسایی شوند. داده‌هایی مانند اطلاعات جمعیت‌شناختی مخاطبان، تاریخچه فعالیتها، اطلاعات مربوط به تولید، این که چگونه مخاطبان محصولات را مورداستفاده قرار می‌دهند، این که تمایل دارند از چه سطحی از خدمات استفاده کنند، میزان رضایت آن‌ها از پشتیبانی محصولات و یا حتی شکایت‌هایی که ممکن است از خدمات و محصولات داشته باشند، همچنین اطلاعات مربوط به تحقیقات از بازارهای سنتی، باید در این طرح تعریف و دسته‌بندی و شناسایی شوند. در مرحله بعد باید نحوه مدیریت و تحلیل این داده‌ها تعریف و اجرا گردد. در حال حاضر تقریبا هیچکس در معاونت نمی داند که با این داده‌ها چه باید بکند و یا حتی آن را چگونه تحلیل کند. چراکه این داده‌ها معمولاً به روشی درست و کاربردی جمع‌آوری و ذخیره‌سازی نشده‌اند. اغلب آن‌ها به‌صورت خام هستند. این داده‌ها فهرست‌شده و در حال استفاده نیستند. حتی بسیاری از کارشناسان و یا مدیران از وجود آن‌ها آگاه نیستند؛ اما درمجموع کارشناسان معتقدند که هرگونه اطلاعاتی که به شما اجازه دهد که بین خود و مخاطبان و یا میان مشتریان‌تان ارتباط برقرار کنید، حتماً از ظرفیت بالایی برخوردار خواهد بود. داده تاریک به معاونت اجازه می‌دهد که تصویری دقیق از مخاطبان و مشتریان خود کسب کنند تا بتوانند بهترین پیشنهادها را به آن‌ها ارائه دهند. این امر موجب رونق کسب‌وکار و فعالیت‌ها و خدمات و ارتباط بهتر میان مشتری و مخاطب و معاونت خواهد شد.

شرح نیاز فناورانه

عنوان	سامانه امن پشتیبان گیری و بازیابی داده ها
شرح	تهیه نسخه پشتیبان با دو هدف صورت می‌گیرد. اولین هدف آن بازیابی داده اصلی پس از از بین رفتن داده مانند حذف یا خرابی داده است. دومین هدف پشتیبان گیری، بازیابی داده از زمان‌های قبلی با توجه به خط‌مشی نگهداری داده‌ی کاربر است. در برنامه پشتیبان گیری مشخص می‌شود که نسخه‌های داده برای چه مدت نگهداری شوند. ازآنجایی‌که سیستم پشتیبان دارای حداقل یک کپی از تمامی داده‌هایی است که ارزش ذخیره‌سازی را دارند، الزامات ذخیره‌سازی داده قابل توجه است. سازمان‌دهی این فضاهای ذخیره‌سازی و مدیریت فرآیند پشتیبان گیری، امری پیچیده است. برای یک راه حل پشتیبان گیری ارزشمند، باید عواملی مانند ویژگی‌های فیزیکی و دوره گردش در نظر گرفته شده و مدیریت شوند. در طرح سیستم داخلی و امن پشتیبان گیری و بازیابی داده‌ها، علاوه بر مشخص نمودن نوع و تعداد رسانه‌های پشتیبان گیری، مدل‌های مخزن داده موردنیاز نیز باید مشخص گردد. برخی از مهم‌ترین این مدل‌ها عبارتند از: ❖ مخزن بدون ساختار ❖ مخزن کامل / تصویربرداری از سیستم ❖ مخزن سبک افزایشی ❖ مخزن سبک دلتای معکوس

شرح نیاز فناورانه

عنوان	تکمیل و توسعه گروه واکنش سریع به رخدادهای رایانه ای (CERT)
شرح	اهداف طرح تکمیل و توسعه گروه واکنش سریع به رخدادهای رایانه ای (CERT) عبارتند از: ❖ کاهش و به حداقل رساندن بروز حادثه در حوزه شبکه‌های رایانه‌ای ❖ کاهش و به حداقل رساندن زمان پاسخ به حوادث در حوزه شبکه‌های رایانه‌ای ❖ کاهش و به حداقل رساندن میزان خسارت حوادث در حوزه شبکه‌های رایانه‌ای اهم موارد مدنظر جهت تکمیل و توسعه گروه واکنش سریع به رخدادهای رایانه ای (CERT) عبارت است از: ❖ طراحی سرویس‌های گروه واکنش سریع به رخدادهای رایانه ای ❖ طراحی زیرساخت گروه واکنش سریع به رخدادهای رایانه ای ❖ استقرار و پیاده‌سازی گروه واکنش سریع به رخدادهای رایانه ای ❖ راه‌اندازی گروه واکنش سریع به رخدادهای رایانه ای و نظارت بر بهره‌برداری ❖ بهره‌برداری و ارتقا گروه واکنش سریع به رخدادهای رایانه ای

شرح نیاز فناورانه

عنوان	طراحی و پیاده‌سازی آزمایشگاه ارزیابی امنیتی نرم افزار و سخت‌افزار
شرح	یکی از خدمات اصلی آزمایشگاه ارزیابی امنیتی نرم افزار و سخت افزار، اجرای روال ارزیابی امنیتی محصولات فناوری اطلاعات بوده که به تبع آن گزارش فنی در خصوص میزان تطبیق یک محصول با سند هدف امنیتی مرتبط منتشر خواهد شد. صدور گواهینامه امنیتی برای محصولات توسط آزمایشگاه و مراجع معتبر بر اساس نتایج ثبت شده به انجام می‌رسد. در طی فرآیند ارزیابی، اسناد تولید کننده مطابق با روال ارزیابی بررسی و تکمیل شده و متناسب با اسناد ارائه‌شده توسط تولید کننده و بررسی الزامات بر روی محصول نصب

شرح نیاز فناورانه

عنوان	تدوین طرح های امنیت سازمانی مبتنی بر استاندارد ها و رویکرد های نوین
شرح	طرح تدوین استراتژی امنیت سایبری معاونت طرح تدوین سند سیاست امنیت سایبری معاونت طرح مدیریت یکپارچه مخاطرات امنیت سایبری طرح تدوین، اجرا و ارزیابی آموزش‌ها و مهارت‌های تخصصی امنیتی سایبر کارکنان طرح تدوین دستورالعمل‌ها و آئین‌نامه های حوزه امنیت سایبر طرح طراحی و تدوین تداوم کسبوکار طرح تدوین اقدامات و راهکارهای امنیت سایبری (مدیریت تغییر، استانداردها و راهنما ها، فهرست بندی دارائی‌ها) طرح مطالعه و شناسایی متدولوژی‌ها و ابزارهای ارزیابی آسیبپذیری امنیتی طرح طراحی، بازمهندسی و اجرای فرآیند های امنیت سایبر طرح بازیابی رخدادهای فاجعه آمیز سایبری طرح ملاحظات امنیتی مرتبط با تأمین‌کنندگان محصولات و خدمات سایبر طرح تأمین و توسعه نیروی انسانی ماهر و با تجربه

حوزه فناوری تقاضا

امنیت نرم‌افزار، امنیت شبکه، امنیت سامانه ها، امنیت سازمانی

حوزه صنعتی تقاضا

شرکت‌های تخصصی توسعه دهنده نرم‌افزارهای امن، شرکت‌های تخصصی امنیت شبکه، شرکت های تخصصی توسعه دهنده سیستم های امن، شرکت های تخصصی ارائه دهنده خدمات امنیت

پارامترهای عملکردی لازم (الزامات راه‌حل‌های پیشنهادی)

قابلیت امنیت نرم افزار

قابلیت امنیت شبکه

دارای پایگاه دانش از الگوی آزمون‌های امنیتی

شناخت نسبت به زیرساخت های رسانه

فناوری‌ها و راه‌حل‌های نامطلوب

فناوری‌های غیر نوآورانه و غیر خلاقانه

مدل همکاری مطلوب

مشارکت

خرید

سرمایه‌گذاری