سامانه مدیریت پدافند غیر عامل شبکه‌های رایانه‌ای

دکتر حسین شیرازی
روح الله کاری

چکیده

مهم‌ترین وظیفه مدیران تصمیم گیری در شرایط متفاوت می‌باشد و در حقیقت مدیریت چیزی جز تصمیم گیری نیست. با توجه به اینکه تصمیم‌گیری در حوزه فن‌آوری اطلاعات و به خصوص امنیت آن دارای پیچیدگی‌های خاص خود می‌باشند و عوامل موثر بر آن گسترده و متفاوت است، استفاده از سامانه‌های تصمیم‌یار یکی از بهترین پیشنهادات برای رفع معضلات مدیریتی در این حوزه می‌باشند. به منظور ایجاد سهولت در تصمیم‌گیری در موارد ساخت‌نیافته فن‌آوری اطلاعات مانند امنیت سامانه تصمیم‌یار با رویکرد «چه خواهد شد اگر» در این مقاله پیشنهاد می‌شود.

هدف این مقاله ارائه طراحی جهت تولید یک سامانه تصمیم‌یار صفحه گسترده با رویکرد تهدید محور، برای تحلیل مخاطرات امنیتی و تهدیدات سایبری با رویکرد پدافند غیر عامل می‌باشد. این سامانه در سطح کاربردی از نوع غیر فعال می‌باشد که مستقیماً توصیه‌ای برای تصمیم‌گیری ارائه نمی‌دهد؛ و با توجه به انواع ورودی خروجی‌های متفاوتی را ارائه می‌دهد و تصمیم گیری نهایی را به مدیر مسئول محول می‌نماید. جهت طراحی سامانه باید آسیب‌های شبکه‌های رایانه‌ای و نحوه مقابله با آن‌ها را شناسایی نمود سپس با توجه به مؤلفه‌های پدافند غیرعامل و امنیت کاربرد هر یک از آسیب‌پذیری‌ها را مشخص نموده و در پرسشنامه‌ای که بر اساس کاربرد هر یک از موارد چک‌لیست وزن مورد نظر لحاظ گردد و سپس در هر شبکه مورد سنجش قرار گیرد.

کلمات کلیدی:

سامانه‌های مدیریت، سامانه‌های پشتیبانی از تصمیم، پدافند غیرعامل، شبکه‌های رایانه‌ای، امنیت، آسیب‌پذیری‌های امنیتی.

۱- مقدمه

سامانه‌های رایانه‌ای هرچند باعث گستردگی ارتباطات و تسریع در فرایند عملیات‌ها درون سازمان‌ها شده‌اند لیکن تهدیدات گسترده‌ای را نیز به همراه دارند. با توجه به گسترش روزافزون شبکه‌های رایانه‌ای و قابلیت اتصال این شبکه‌ها در سطوح مختلف آسیب‌پذیری‌ها و تهدیدات این حوزه نیز گسترش یافته و جلوه بین‌المللی پیدا کرده‌اند.

نکته قابل توجه در فضای سایبری این است که حملاتی که امروزه صورت می‌پذیرد خسارات مادی و معنوی بسیار گران‌تری نسبت به حملات گذشته از خود برجای می‌گذارد. بدین معنی که این‌گونه خسارات علاوه بر خسارات مالی برجای گذاشته، سبب ایجاد اختلال در کارایی شبکه‌ها، اختلال در نظام گردش اطلاعات سازمان‌ها و از همه مهم‌تر سلب اعتماد بسیاری از اقشار جامعه نسبت به سازمان-هایی که مورد هجوم واقع گردیده‌اند، می‌شود. به عنوان نمونه چنانچه شبکه رایانه‌ای یک بانک مورد حمله الکترونیکی قرار گیرد، در آن صورت میزان اعتماد افراد نسبت به سرمایه‌گذاری در بانک مزبور به طور چشمگیری کاهش می‌یابد. در واقع حملات به شبکه‌های رایانه‌ای در فضای سایبری بزرگ‌ترین آسیب‌ها را به فرایند کسب‌وکار سازمانی وارد نموده و اعتبار آن‌ها را مخدوش می‌نماید. لذا پرداختن به پدافند غیر عامل و امنیت شبکه‌های رایانه از ضرورت‌های این حوزه بوده و پیش از راه‌اندازی هر گونه خدماتی در بستر فن‌آوری اطلاعات باید امنیت آن مد نظر قرار گیرد.

۲- سامانه‌های مدیریت[1]

سامانه‌های مدیریت ابزارهایی هستند که مدیران را در جهت نیل به اهدافشان یاری می‌نمایند. این سامانه‌ها با جمع‌آوری داده‌ها و نظم دهی به آن‌ها و در برخی از موارد با استخراج اطلاعات و دانش به مدیران در انجام وظایف مدیریتیشان یاری می‌رسانند. این سامانه‌ها وظیفه دارند اطلاعات مناسب و مربوط را ارائه دهند. این سامانه‌ها در حل مشکلات ساخت نیافته، نیمه ساخت یافته و یا مشکلات ساختار یافته کاربرد دارند. با توجه به محل استفاده از آن‌ها درجه‌ای از هوشمندی را در خود دارند. از مهم‌ترین این سامانه‌ها، سامانه‌های پشتیبانی از تصمیم[2] یا تصمیم‌یار می‌باشند.

1 - management systems
2 - DSS Decision Support Systems

۲-۱- سامانه‌های تصمیم‌یار.

تصمیم‌گیری مترادف اداره کردن است. تصمیم گیرنده فردی است که آماده است در تقاطع در یکی از مسیرها پا بگذارد. تصمیم گیری یکی از مهم‌ترین فرآیندهای مدیریت می‌باشد. صاحب‌نظران علم مدیریت می‌گویند، مدیریت چیزی جز تصمیم گیری نیست. سامانه‌های پشتیبانی از تصمیم یک مجموعه از رویه‌ها را در مدل مشخص برای پردازش داده و کمک به مدیران در تصمیم گیری بیان می‌کند. سامانه پشتیبانی از تصمیم یک «سامانه مدل‌سازی[3]» است، یعنی باید ابتدا کد مجازی آن نوشته شود. واحد عملیاتی در سامانه پشتیبانی از تصمیم پرس و جو[4] که فقط می‌تواند واکشی داده را انجام دهد است و امروزه مبتنی بر دانش می‌باشد. سامانه پشتیبانی از تصمیم می‌تواند دو رویکرد " چه خواهد شد اگر[5]" و یا "جستجوی هدف[6]" را داشته باشد. [۲].به عنوان یک تعریف کلی می‌توان گفت سامانه تصمیم‌یار یک سیستم متعامل، انعطاف‌پذیر و وفق پذیر است که به طور ویژه برای پشتیبانی از راه حل مشکلات مدیریتی ساختار نیافته جهت تصمیم‌گیری بهتر، توسعه یافته است. این سیستم از داده‌ها استفاده می‌کند، رابط کاربر ساده‌ای فراهم می‌کند و می‌تواند دیدگاه تصمیم گیرندگان را هم در تصمیم‌گیری شرکت دهد.

۲-۲- دسته بندی‌های سامانه‌های تصمیم‌یار:

دسته بندی‌های مختلفی برای سامانه‌های پشتیبانی از تصمیم تعریف شده است از جمله آن‌ها هالس‌اپل[7] و وینس‌تون[8] است که در سال ۱۹۹۶ به صورت شش قالب تعریف شده است :

۱. **متن‌گرا[9] :** اطلاعات به صورت متن ذخیره شده‌اند و بایستی در دسترس کاربر باشد.
۲. **پایگاه داده گرا:** به جای سازماندهی متن، داده‌ها با ساخت یافتگی بالایی، سازماندهی می‌شوند.
۳. **صفحه گسترده‌گرا:** صفحه گسترده، زبان مدل‌سازی است که به کاربر امکان می‌دهد برای تجزیه و تحلیل

3 - Modeling System
4 - Query
5 - What If
6 - Goal Seeking
7 - Halsapple
8 - Whinston
9 - Text Oriented

سامانه‌های پشتیبانی از تصمیم مدل‌ها را بنویسد. در این نوع نه تنها دانش رویه‌ای وجود دارد، بلکه به سیستم فرمان می‌دهد دستورهای داخلی صفحه گسترده را نیز اجرا کند. این سامانه‌ها حالت خاصی از سامانه‌های پشتیبانی از تصمیم حل‌گرا است.

۴. **حل‌گرا:** مثل رویه مقدار سفارش اقتصادی برای محاسبه میزان سفارش بهینه. الگوریتم یا رویه‌ای رایانه‌ای وجود دارد که به منظور حل نوع خاصی از مسئله، محاسبات ویژه‌ای انجام می‌دهد.

۵. **قانون‌گرا:** در بخش دانش، قواعد و قوانین و رویه‌ای استنباطی یک سیستم خبره قرار دارند. این قوانین حالت کمی و کیفی دارند.

۶. **ترکیبی**: سیستمی پیوندی است که یک یا چند جزء، از ساختارهای بالا را در خود جای داده است.[۳]

۳- پدافند غیر عامل[1] در حوزه سایبر

اقدام غیر مسلحانه‌ای که موجب کاهش آسیب‌پذیری نیروی انسانی، ساختمان‌ها، تأسیسات، تجهیزات، اسناد و شریان‌های کشور در مقابل عملیات خصمانه و مخرب دشمن گردد، پدافند غیرعامل گفته می‌شود. پدافند غیرعامل شامل کلیه اقدامات به منظور حفظ امنیت، ایمنی و پایداری شبکه و تجهیزات وابسته به شبکه می‌باشد.پدافند غیرعامل مجموعه اقداماتی است که انجام می‌شود تا در صورت بروز جنگ، خسارات احتمالی به حداقل میزان خود برسد. [۴]. اقدامات انجام شده برای کاهش احتمال وقوع و به حداقل رساندن اثرات خسارت‌های اقدامات خصمانه بدون گرفتن ابتکار عمل، ایجاد می‌شود. امنیت سایبری مؤثر باید شامل برخی از انواع پاسخ فعال به بعضی از تهدیدات جهت ایجاد هزینه‌ای بالاتر از هزینه‌ای که فرد مهاجم حاضر به پرداخت آن است می‌باشد. دفاع غیرعامل در واقع مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت گیرد. چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب‌دیده را با کم‌ترین هزینه فراهم می‌سازد. [۵]

جلوگیری[2] عبارت از شناسایی راه‌های نفوذ و حمله و مقابله با آن‌ها جهت افزایش ضریب امنیت، ایمنی و پایداری است. به‌کارگیری تمهیدات و ملاحظات پدافند غیرعامل علاوه بر کاهش شدید هزینه‌ها، کارایی دفاعی طرح‌ها، اهداف و پروژه‌ها را در زمان تهاجم دشمن بسیار افزایش خواهد داد؛ و در عین حال باعث جلوگیری نیز می‌شود. هدف از اجرای طرح‌های پدافند غیرعامل کاستن از آسیب‌پذیری نیروی انسانی و تأسیسات و تجهیزات حیاتی و حساس و مهم کشور علیرغم حملات خصمانه و مخرب دشمن و استمرار فعالیت‌ها و خدمات زیربنایی و تأمین نیازهای حیاتی و تداوم اداره کشور در شرایط بحرانی ناشی از جنگ است. به عنوان مثال، از پدافند غیرعامل می‌توان به استتار، اختفا و ایجاد سرپناه برای تأسیسات مهم و استراتژیک اشاره کرد. در پدافند غیرعامل تمام نهادها، نیروها، سازمان‌ها، صنایع و حتی مردم عادی می‌توانند نقش مؤثری بر عهده گیرند. انجام اقدامات دفاع غیرعامل، در جنگ‌های نامتقارن امروزی در جهت مقابله با تهاجمات خصمانه و تقلیل خسارت ناشی از حملات سایبری، موضوعی بنیادی است تا حدی که حفظ امنیت ملی و اقتصادی، شکست‌ناپذیری در جنگ نرم، به نحو چشمگیری وابسته به برنامه‌ریزی و ساماندهی همه جانبه در موضوع حیاتی دفاع غیرعامل می‌باشد. با فراگیری حوزه فن آوری اطلاعات و تطبیق آن با دنیای واقعی کلیه این تهدیدات به این حوزه نزدیک شده‌اند. در عین حال آفند در این حوزه مستلزم هزینه چندانی نمی‌باشد و نیاز به حضور فیزیکی در محل جنگ ندارد. در حال حاضر مهم‌ترین مراکز مالی دنیا از طریق اینترنت و در هر محلی از جهان قابل دسترس می‌باشد؛ که باعث افزایش اهمیت پدافند غیرعامل در این حوزه شده است.[۶]

۴- امنیت در فضای سایبری

در تعریف امنیت گفته شده است که، امنیت عبارت است از در معرض خطر نبودن و یا از خطر محافظت شدن. همچنین عبارت است از رهایی از تردید، آزادی از اضطراب و بیمناکی و داشتن اعتماد و اطمینان موجه و مستند. [۷] و این بدان معناست تا زمانی که تهدیدی وجود دارد فقدان امنیت نیز وجود دارد. امنیت در فضای سایبری بر اساس عدم وجود تهدیدات می‌باشد که این تهدیدات از طرف هکرها، نرم افزارهای مخرب، کارمندان ناراضی، رقیبان و دیگر

1 - Passive defense

2 - Prevention

منابع داخلی و خارجی به وجود می‌آیند. بدیهی است در سازمان-هایی که از حساسیت بیشتری برخوردار بوده و اطلاعات دارای ارزش بیشتری می‌باشند، مسئله دفاع از حریم اطلاعات و دارایی‌ها از اهمیت بالاتری برخوردار می‌گردد.

۴-۱- تهدیدات فضای سایبری

معمولاً حملاتی که به شبکه‌ها می‌شوند نتیجه وجود آسیب‌پذیری و نقاط ضعف در شبکه می‌باشد. این گونه نقاط ضعف می‌توانند حاصل یک طراحی ضعیف و یا برنامه‌ریزی ضعیف در شبکه باشد. امنیت سایبری به شکل حفاظت از داده‌های یک سیستم در مقابل افشاسازی، تغییر یا تخریب غیرمجاز و حفاظت از خود سیستم رایانه در مقابل استفاده، تغییر یا نفی خدمت غیرمجاز تعریف می‌شود. جهت مقابله با این تهدیدات اقدامات پراکنده امنیتی و با توجه به سلایق مدیران و مسئولان امنیت شبکه انجام می‌شود، لذا داشتن طرحی جامع و هماهنگ برای مقابله با این تهدیدات امری ضروری است. تمامی تهدیدات فضای سایبری سه اصل اساسی امنیت به شرح زیر را مورد تهدید، قرار می‌دهند:

محرمانگی[1]: حفاظت از داده‌های یک سیستم به شکلی که افراد غیرمجاز نتوانند به این اطلاعات دسترسی داشته باشند است.

جامعیت، تمامیت، یک‌پارچگی[2]: به معنای حفاظت داده‌های سیستم در مقابل تغییرات غیرمجاز سهوی یا عمدی است.

دسترس‌پذیری[3]: عبارتست از اطمینان از اینکه یک سیستم کامپیوتری هر زمان که لازم باشد توسط کاربران مجاز قابل دسترسی باشد. [۸].

معمولاً حملاتی که به شبکه‌ها می‌شود نتیجه وجود آسیب‌پذیری و نقاط ضعف در شبکه می‌باشد. این گونه نقاط ضعف می‌توانند حاصل یک طراحی ضعیف و یا برنامه‌ریزی ضعیف در شبکه باشد.

۴-۲- ضعف‌های فن آوری اطلاعات

به منظور انجام اقدامات پدافند غیر عامل در شبکه‌های رایانه‌ای که باعث ایجاد امنیت نسبی در فضای سایبری شده و با استفاده از سامانه‌های امن ساز می‌توان حداقل سطح امنیت را برای شبکه‌های رایانه‌ای فراهم آورد. به این منظور باید ریشه آسیب‌پذیری‌های موجود در فضای سایبری را شناسایی نمود. ریشه بسیاری از مشکلات و آسیب‌پذیری‌های امنیتی را می‌توان در سه ضعف عمده، فن‌آوری، پیکربندی و سیاست‌ها جستجو کرد.ضعف فناوری به مواردی همچون پروتکل‌ها، سیستم‌های عامل و سخت افزارها مرتبط می‌گردد. پروتکل‌ها، سیستم‌های عامل و سخت افزار اغلب به صورت پیش فرض ایمن نمی‌باشند. در واقع، ضعف در فناوری به عدم وجود شرایط مطلوب امنیتی در حوزه‌های سخت افزاری و نرم افزاری مربوط می‌گردد. پیکره بندی توسط عوامل انسانی همواره توأم با خطا بوده و همچنین پیکربندی پیش فرض اغلب تجهیزات مورد استفاده در شبکه‌های رایانه‌ای ضعف‌های امنیتی مشهودی دارند. سیاست‌های امنیتی در یک شبکه، نحوه و زمان پیاده سازی امنیت در شبکه را تشریح می‌نمایند. عدم تدوین یک سیاست امنیتی مدون می‌تواند زیرساخت فناوری اطلاعات و ارتباطات یک سازمان را با مشکلات امنیتی مواجه نماید.

۵- سامانه‌های امن ساز (پدافند غیرعامل) در فناوری اطلاعات

سامانه‌های امن ساز، سامانه‌هایی هستند که به منظور تأمین امنیت از آن‌ها استفاده می‌شود. این سامانه‌ها در حوزه‌های مختلفی کاربرد دارند برای مثال در حوزه حفاظت فیزیکی سامانه‌های امن ساز شامل دوربین‌های مدار بسته، سیستم‌های اعلام و اطفاء حریق و ... می‌باشند. این سامانه‌ها در حوزه کنترل دسترسی و احراز اصالت سامانه‌های امن ساز شامل کارت‌های هوشمند، بیومتریک و... می‌باشند.

در حوزه فناوری اطلاعات این سامانه‌ها دارای تنوع گسترده‌ای بوده و هر یک از آن‌ها جهت مقابله با آسیب‌پذیری‌های خاصی مورد استفاده قرار می‌گیرند. سامانه‌های امن ساز برای محیط فناوری اطلاعات به صورت اجمالی عبارتند از ضد بد افزارها، دیواره آتش، سامانه‌های مدیریت یک‌پارچه‌ی تهدیدات[4]، رمز کننده، سامانه‌های آشکارسازی حملات، سامانه انسداد حملات، سامانه‌های کندوی عسل.

1 - Confidentiality
2 - Integrity
3 - Availability

4 – UTM : Unified Threat Management

۵-۱-۱- مشکلات سامانه‌های امن ساز

همان‌گونه که اشاره شده ضعف‌های موجود در فضای سایبری را می‌توان به ضعف فن‌آوری، ضعف پیکربندی، ضعف سیاست‌ها تقسیم نمود. به طور مشخص سامانه‌های اشاره شده در بالا بیشتر تلاش خود را در حل نمودن ضعف‌های فناوری اطلاعات می‌نمایند. و در مقابل ضعف‌های پیکره بندی و سیاست‌ها عملکردی خنثی دارند در حقیقت نه تنها آن‌ها را بر طرف نمی‌نمایند بلکه قدرت شناسایی آن‌ها را ندارند. به طور کلی مشکلات سامانه‌های امن ساز عبارتند از:

- ✓ نیاز به داشتن دانش فنی (در برخی از این محصولات) جهت پیکره بندی و بهره برداری امنیتی.
- ✓ عدم ارائه راه حل برای مواردی جدید و پیش بینی نشده(از پیش تعریف نشده).
- ✓ نبود هوشمندی در عملکرد و تعاملی نبودن اکثر آن‌ها.
- ✓ عدم اعمال سیاست‌های امنیتی سازمانی.
- ✓ توجه به یک جنبه خاص از امنیت.
- ✓ نیاز به به‌روز رسانی.

سامانه‌های امن ساز توانایی ایجاد امنیت تنها برای ضعف‌هایی از نوع فناوری اطلاعات را دارا می‌باشند. و در مقابل ضعف‌های پیکره‌بندی و سیاست‌های سازمانی توانایی چندانی ندارند.

۶- سامانه پیشنهادی

این سامانه تلاش دارد با ترکیب توانمندی‌های فنی که در سامانه‌های امن ساز رایج وجود دارد در قالب سامانه‌های مدیریتی، نقاط ضعف موجود در سامانه‌های امن ساز معمولی را بر طرف نماید و به برخی از پرسش‌های مطرح شده در بحث پدافند غیر عامل پاسخ گوید.

این سامانه با احصاء وضعیت جاری که بر اساس خود اظهاری مدیران امنیت شبکه است، نموداری را ترسیم می‌نماید. پس از مشخص نمودن وضعیت جاری مسئولین مرتبط با توجه به توانمندی‌های خود در اقدامات آتی جهت تبدیل این مشکلات به وضعیت غیر مرتبت و یا حذف آن را نیز اظهار می‌نمایند. که در نمودار نهایی قابل مقایسه خواهد بود با هر تغییر در میزان وضعیت هدف می‌توان نزدیک شدن به سطح امنیت دلخواه را مشاهده نمود. این سامانه با تکیه بر پایگاه دانشی خود که توسط کاربران خاص قابل توسعه می‌باشد سعی در تشخیص علل مشکلات امنیتی با توجه به وزن آن‌ها در شبکه را دارد. پاسخگویی به پرسش‌های این بانک باعث مشخص شدن اکثر وجوه نقاط ضعف امنیتی که در حالت عادی از منظر توجه مخفی می‌مانند می‌شود. با عنایت به این نکته که در پایگاه دانشی این سامانه حوزه‌های مشکلات و آسیب‌پذیری‌ها در شبکه‌های رایانه‌ای مشخص شده‌اند پاسخ گو در جواب به سؤالات بدون توجه به این موضوع که سؤال در چه حوزه‌ای می‌باشد به صورت ناخواسته حوزه امنیت را مشخص می‌نماید. یکی از اساسی‌ترین مشکلات بر طرف نمودن آسیب‌های شبکه‌های رایانه‌ای بلا تکلفی و سر در گمی برای اقدامات مورد نیاز می‌باشد.

۷- پایگاه دانشی سامانه (آسیب‌های شبکه‌های رایانه‌ای و نحوه مقابله با آن‌ها)

حملات به شبکه‌های رایانه‌ای طیف گسترده‌ای را شامل می‌شود که پرداختن به همه آن‌ها از فرصت این مقاله فراتر می‌باشد لیکن به سبب اهمیت موضوع و پشتیبان علمی سامانه در بررسی وضعیت پدافند غیر عامل فضای سایبری و همچنین جهت نزدیک شدن ذهن به این موضوع به برخی از مهم‌ترین آن‌ها که خود دارای زیر مجموعه‌های زیادی می‌باشند اشاره شده است.

در این بخش مقاله موارد اصلی پایگاه دانشی طراحی سامانه مطرح می‌شوند که در آن مهم‌ترین آسیب‌های مطرح به صورت اجمالی و با رعایت اختصار مورد بررسی قرار می‌گیرند و همچنین به منظور امن نمودن آن‌ها راهکارهایی ارائه می‌شود. آسیب‌های مطرح در این حوزه بر اساس مؤلفه‌های امنیت دسته بندی می‌شوند. سپس ضریب مورد نظر توسط طراح سامانه با توجه به حوزه نفوذ و نوع کاربرد شبکه به آن‌ها داده می‌شود. در نهایت حوزه عملکردی هر آسیب پذیری بر اساس زمان وقوع مشخص می‌گردد. برای مقابله با حملات سایبری و پدافند غیر عامل روش‌هایی متناسب با نوع حملات وجود دارد که محدوده وسیعی از اقدامات و تجهیزات را شامل می‌شود. در زیر به برخی از مهم‌ترین آسیب‌های فضای سایبری و نحوه مقابله با آن‌ها پرداخته شده است.

۷-۱- حمله جلوگیری از خدمات.

مهم‌ترین و شایع‌ترین حمله در فضای سایبری حمله منع خدمات می‌باشد در عین حال این حمله از گستردگی و تنوع زیادی در بین انواع حملات به شبکه‌های رایانه‌ای برخوردار می‌باشد. حمله جلوگیری خدمات از لحاظ گونه به دو دسته کلی DOS و حمله

جلوگیری از خدمات توزیع شده[1] تقسیم می‌شود. امروزه ساز و کارهای توانمندی برای مقابله با این حمله وجود دارد، این حملات هنگامی رخ می‌دهد که اطلاعات به طور سیل‌آسا از سوی حمله کننده به شبکه ارسال گردد. هر مؤلفه‌ای که به نوعی به شبکه مرتبط و متصل می‌باشد از قبیل رایانامه، سرور DNS و تجهیزات مسیریابی و... ابزار مناسبی برای حمله به شمار می‌روند. مقابله با این حمله شامل تجهیزات و اقداماتی می‌شود که تجهیزات مقابله با این حمله سامانه‌های امنیتی مانند دیواره‌های آتش، سامانه تشخیص و جلوگیری از نفوذ و... می‌باشد و همچنین مجموعه‌ای از اقدامات شامل انجام تنظیمات امنیتی، تفکیک و مشخص نمودن حدود دسترسی و ... می‌باشد. [۹]

۷-۲- حمله استراق سمع[2]

در این حملات شخص مهاجم هیچ‌گونه اثری بر روی روند نقل و انتقال اطلاعات در سطح شبکه نمی‌گذارد بلکه اقدام به جمع‌آوری اطلاعات می‌نماید. منشأ اصلی این‌گونه حملات نفوذ شخص مهاجم در مسیر ارتباطی شبکه و امکان ردگیری بسته‌های اطلاعاتی در حال تبادل در شبکه است. حمله شنود یکی از فراگیرترین روش‌های به - دست آوردن بسته‌ها و فریم‌های اطلاعاتی در شبکه‌ها محسوب می‌شود. در اکثر حملاتی که به شبکه‌ها صورت می‌گیرد، حمله شنود جزء حملات مقدماتی جهت کسب اطلاع از وضعیت ترافیک شبکه و هم‌چنین کسب اطلاع از محیط شبکه صورت می‌باشد. مناسب‌ترین راه دفاع در برابر حمله شنود، استفاده از روش رمزنگاری اطلاعات است. البته رمزنگاری داده‌ها از سرقت اطلاعات جلوگیری به عمل نمی‌آورد، بلکه اطلاعات مزبور را برای شخص مهاجم نامفهوم می‌گرداند. یکی دیگر از راه‌های مقابله با حمله شنود، ایجاد محرمانگی در داده‌ها با استفاده از توابع درهم سازی[3] می‌باشد. [۱۰]

۷-۳- حمله سرریز بافر[4]

دلایل عمده وقوع این حمله وجود ضعف در ساخت برنامه‌های نرم-افزاری است. این‌گونه برنامه‌های نرم‌افزاری ممکن است دارای اشکالات و نواقصی از جمله سرریز ناحیه پشته[5]، یا خطا و اشکال در ناحیه توده[6]، خطا در قالب رشته‌های ورودی می‌باشد. حمله سرریز ناحیه پشته با ورودی نادرست و کنترل نشده بر سیستم رخ می‌دهد. به گونه‌ای که ورودی نادرست باعث ایجاد تغییرات ناخواسته در اجرای برنامه‌ها می‌گردد. بنابراین در برنامه‌هایی که در آن‌ها طول متغیرهای ورودی به سیستم توسط نرم‌افزار کنترل نمی‌گردند، باعث ایجاد سرریز در حافظه و بروز این‌گونه حملات می‌شود. اصلی‌ترین روشی که با این حمله مقابله می‌کند تکنیک Buffer Overflow Mutation نامیده می‌شود.[۹]

۷-۴- حمله جعل هویت.

در این حمله شخص مهاجم، هویت و اعتبار نامه کسی را ارائه می‌کند که در واقع مالک آن نیست. این دسته از مهاجمین به طرق مختلف اقدام به حمله جعل هویت می‌کنند. نفوذگر در اثر اجرای حمله جعل هویت قادر به انجام برخی امور در شبکه از جمله ایجاد تغییر در داده‌ها[7]، تزریق و ایجاد ترافیک جعلی در سطح شبکه می‌باشد. در اثر حمله جعل هویت، نفوذگر قادر به انجام هرگونه اقدام غیرمجاز و خرابکارانه در سطح شبکه می‌باشد. زیرا وی در اثر این حمله در واقع کلیه موانع موجود بر سر راه "روابط اعتماد" را دور زده و پشت سر گذارده است. یکی از اساسی‌ترین راه‌های مقابله با حمله جعل هویت بهره‌گیری از روش‌ها و مکانیزم‌های رمزنگاری اطلاعات احراز هویت می‌باشد. مکانیزم دیگر برای مقابله با این حمله، به‌کارگیری سرویس‌های "عدم انکار" در تبادل اطلاعات در شبکه می‌باشد. [۱۰]

۷-۵- حمله به سرورهای وب و برنامه‌های تحت وب.

یک سرویس دهنده وب در یک حمله خود می‌تواند به عنوان یک درگاه ورودی به شبکه داخلی محسوب شود. چنانچه یک سرویس دهنده وب سقوط کند، تمامی سرویس‌ها و نرم‌افزارهای نصب شده در آن نیز در معرض حمله واقع می‌گردند. برخی نقاط ضعف سرویس دهنده‌های وب که احتمال حمله به آن‌ها را افزایش می‌دهند به قرار زیر می‌باشند:

1- DDOS Distributed Denial Service
2- Sniffing attacks (Interception attacks)
3- Hash Functions
4- Buffer Overflow
5- Stack Overflow
6- Heap
7- Modification

پیکربندی نامناسب نرم‌افزارهای نصب شده بر روی سیستم. وجود خطاهای[1] نرم‌افزاری در نرم‌افزارهای کاربردی. وجود ضعف در کدهای برنامه‌ها. عدم تنظیم مناسب سیستم‌عامل‌ها و برنامه‌ها. ضعف و یا فقدان مدیریت وصله‌ها[2]. عدم به روز آوری آن‌ها در مواقع مناسب. عدم وجود سیاست‌های امنیتی کامل، دقیق و برنامه‌ریزی شده در شبکه. وجود ارتباط مستقیم بین وب سرورها و شبکه داخلی که حاوی اطلاعات مهم و طبقه‌بندی است.

یکی از روش‌های مقابله با این‌گونه حملات، مدیریت وصله‌ها می‌باشد. غیر فعال کردن کنترل از راه دور. استفاده از دیوار آتش بین سرویس دهنده وب و شبکه جهانی اینترنت. جایگزین روش get با Post به هنگام ارسال داده به سرویس دهنده وب. از روش‌های امن سازی می‌باشند. [۱۱]

۷-۶- حمله به گذرواژه.

تکنیک‌های شکستن گذرواژه، مکانیزم‌هایی هستند که توسط مهاجمین برای رمزشکنی گذرواژه‌ها و یا از کار انداختن آن‌ها به کار می‌روند. حمله دیکشنری به گذرواژه، اولین قدم تهیه یک لیست از گذرواژه‌ها و کلمات موجود در دیکشنری توسط مهاجم می‌باشد. برای حمله به گذرواژه از حمله شنود در شبکه‌ها و سرقت گذرواژه از SAM[3] نیز استفاده می‌شود. روش دیگر اجرای حمله Brute force می‌باشد که برای رمزشکنی گذرواژه‌های ترکیبی مورد استفاده قرار می‌گیرد. در این روش کلیه ترکیبات حروف، اعداد و علائم با طول-های متفاوت مورد آزمون قرار گرفته تا گذرواژه شکسته شود. یکی از اصولی که می‌بایست در خصوص حفاظت از گذرواژه‌ها علاوه بر حفاظت‌های فیزیکی و پیرامونی از آن‌ها و هم‌چنین انتخاب گذرواژه‌های مقاوم در برابر حمله رعایت شوند، این است که گذرواژه‌ها تحت هیچ شرایطی به صورت متن واضح از شبکه عبور نکنند. روش دیگر برای امن سازی گذرواژه افزودن مقدار نمک[4] ـ به صورت چند بیت اضافی ـ به سمت چپ و یا راست گذرواژه است.

۷-۷- حمله بدافزارها.

به مجموعه‌ای از نرم افزارهایی که باعث تخریب، افشاء، تغییر در اطلاعات و یا سامانه‌های عامل می‌شوند کدهای مخرب یا بد افزار اطلاق می‌شود این گروه از نرم‌افزارها شامل درب‌های پشتی، اسب‌های تروا، ویروس‌ها، نامه های ناخواسته و کرم‌ها و... می‌باشد. اغلب نرم افزارهای ویروس یاب شناخته شده امروزی، قابلیت مقابله با اسب‌های تروا[5] و سایر بد افزارها را نیز دارا بوده و قادر به شناسایی شناسایی درهای پشتی نیز می‌باشند. هر یک از ویروس‌یاب‌ها قابلیت مقابله با دسته‌ای از ویروس‌ها، اسب‌های تروا و درهای پشتی را دارند.

۸- طراحی سامانه تصمیم‌یار پدافند غیر عامل.

هدف؛ طراحی و تولید یک سامانه تصمیم‌یار صفحه گسترده[6] مبتنی بر What if با رویکرد تهدید محور و از نوع غیر فعال، که برای مخاطرات امنیتی و تهدیدات سایبری با رویکرد پدافند غیر عامل می‌باشد. صفحه گسترده نوعی نرم‌افزار است که برای ساده کردن ورود اطلاعات و انجام محاسبات ریاضی طراحی شده‌اند. در سامانه‌های تصمیم‌یار با رویکرد "چه می‌شود اگر" ابتدا بررسی‌های لازم با انجام تغییرات در ورودی‌ها انجام می‌شود و سپس بهترین خروجی به دست آمده اجرا می‌شود. [۱۲]

انجام آزمایش و خطا در فضای حقیقی متضمن پرداخت هزینه هنگفت و صرف وقت گزافی می‌شود که در برخی از موارد باعث صدمات جبران ناپذیری نیز می‌گردد که بدون در نظر گرفتن میزان تأثیر هر اقدامی انجام آن همواره با اشتباه و خسران همراه خواهد بود در واقع با سیستم واقعی نمی‌توان آزمایشات متعدد انجام داد و پس از انجام آزمایش بهترین خروجی را انتخاب و اجرا نمود. آزمایش با سیستم واقعی، فقط برای یک مجموعه از حالات در زمان قابل اجراست و ممکن است فاجعه‌ای به همراه داشته باشد. سامانه پیشنهادی این مقاله در سطح کاربردی از نوع غیر فعال می‌باشد که مستقیماً توصیه‌ای برای تصمیم‌گیری ارائه نمی‌دهد؛ و با توجه به انواع ورودی خروجی‌های متفاوتی را ارائه می‌دهد و تصمیم نهایی را مدیر مسئول را اخذ می‌نماید. جهت طراحی و پیاده‌سازی سامانه باید بانک دانشی سامانه تشکیل گردد و سپس با توجه به مؤلفه‌های پدافند غیرعامل و امنیت کاربرد هر یک از آسیب‌پذیری‌ها را مشخص

1 - Bugs
2 - Patch Management
3 - Security Account Manager
4 - Salt

5 - Anti Trojan
6 – SS-DSS

نموده و بر اساس وزن مورد نظر در هر شبکه‌ای مورد سنجش قرار داد. این سنجش و وزن دهی باید به گونه‌ای باشد که بر اساس نوع شبکه‌ها مؤلفه‌های امنیت از امتیاز متفاوتی برخوردار گردند. در واقع برای افزایش دقت موضوع به جای تک مؤلفه «امنیت»، سه پارامتر «محرمانگی، یک‌پارچگی و دسترس‌پذیری» جایگزین شده است. جهت شفاف نمودن موضوع ذکر این نکته ضروری است که مؤلفه‌های امنیت دارای وزن برابری برای تمام موارد کاربردشان نمی‌باشند. برای مثال در شبکه‌های محلی که اتصال مستقیم به شبکه جهانی ندارند شاخص محرمانگی دارای بالاترین اولویت و شاخص دسترس‌پذیری دارای پایین‌ترین اولویت می‌باشد؛ و بالعکس برای سرورهایی که بر روی شبکه اینترنت خدمات دهی می‌کنند دسترس‌پذیری از اصول اساسی و اولیه می‌باشد؛ و هر لحظه قطع خدمات آن‌ها معادل یک حمله منع خدمات محسوب شده، از اعتبار جهانی آن‌ها کاسته خواهد شد.

۸-۱- جداول پیاده‌سازی

به منظور پیاده سازی نرم افزار باید اطلاعات ترکیب شده را در قالب جداول پیاده‌سازی ترسیم نمود. این جداول دارای سطرهایی می‌باشند که میزان تأثیرگذاری هر آسیب‌پذیری بر روی سه مؤلفه امنیت را مشخص می‌کند. در این جدول هر آسیب‌پذیری بر اساس نوع عملکرد و تأثیرش بر روی شبکه بررسی شده است. این جداول در سه سطح مورد بررسی قرار می‌گیرند. جدول اشاره شده به صورت پیش فرض آماده شده و در سامانه قرار داده خواهند شد.

- ✓ سطح اول جداول دانشی
- ✓ سطح دوم جداول عملکردی
- ✓ سطح سوم جداول وضعیت بحران

۸-۱-۱- سطح اول جداول دانشی

این جداول در هر سه سطح دارای تعداد نامحدودی [قابلیت توسعه نرم افزار] سطر می‌باشد که در این مقاله بیشترین تمرکز بر روی آسیب‌های عمده شبکه‌ای است، و دارای ۸ ستون می‌باشد که در جدول زیر آمده است. این جداول بر اساس بند ۷ این مقاله توسعه یافته است. در این جداول حوزه تأثیر هر یک از آسیب‌ها مشخص می‌شود که در لایه بیرونی سامانه قابل مشاهده نمی‌باشد. برای مثال عمده حملات منع خدمات تنها در حوزه دسترس‌پذیری موثر می‌باشند و در حوزه های محرمانگی و جامعیت تأثیر ندارند. در این بخش برای هر یک از سؤالات اقدام معادل پدافند غیر عامل دیده شده است. برای مثال جهت مقابله با حمله اشاره شده باید از استتار و اختفا و پوشش بهره جست. سؤالات جمع آوری شده با توجه به گستره وسیع تهدیدات بانک اطلاعاتی سامانه را تشکیل می‌دهد این پایگاه داده به سادگی قابل گسترش بوده و هر تعداد سؤال را می‌توان به آن اضافه نمود و یا از آن حذف کرد. این سؤالات بر اساس کاربردهای وسیع انتخاب شده‌اند. در واقع ترکیب سؤالات و حوزه تأثیرگذاری آن‌ها و حوزه پدافند غیر عاملی که با اتکا به آن می‌توان آن‌ها را برطرف و یا حذف نمود پایگاه دانشی نرم افزار را تشکیل می‌دهد.

ردیف	گروه آسیب پذیری	نام آسیب پذیری	بند مرتبت	توضیحات	پدافند غیر عامل (امنیت)		
					محرمانگی	یکپارچگی	دسترس پذیری

جدول ۸-۱- نمونه خام سطح اول جداول دانشی

۸-۱-۲- سطح دوم جداول عملکردی

سامانه باید دارای دو حالت وضعیت جاری و وضعیت آتی باشد. جداول این سطح علی رقم داشتن ستون‌های سطح قبل دارای ۲ ستون اصلی و ۵ ستون فرعی می‌باشد که به شرح ذیل می‌باشند:

وضعیت جاری: در وضعیت جاری سؤال پرسیده شده دارای سه حالت است :

- ✓ جواب مثبت (در صورت وجود آسیب پذیری)
- ✓ جواب منفی (در صورت عدم وجود آسیب پذیری)
- ✓ جواب Not Applicable (در صورت عدم کاربرد آسیب پذیری)

برای تولید نرم افزار سؤالاتی باید از کاربر سامانه پرسیده شوند که این سؤالات جنبه منفی دارند. در واقع مقادیر مثبت در جواب به

وجود آسیب پذیری است که باعث منفی شدن و نامطلوب بودن آن می‌باشد و این پاسخ‌های مثبت در نهایت محاسبه می‌شوند. جهت به دست آوردن نتیجه نهایی مجموع جواب‌های منفی (پاسخ مثبت به وجود آسیب‌پذیری‌ها) در مقادیر محرمانگی، یکپارچگی و دسترس‌پذیری ضرب می‌شود و جواب هر ردیف که ۰ و ۱ است به دست می‌آید و بر تعداد کل سؤالات تقسیم شده تا درصد نهایی به دست آید. در صورت جواب "عدم کاربرد" سؤال از تعداد کل سؤالات حذف شده و مقادیر به دست آمده بر تعداد جدید تقسیم می‌شود. در صورت وجود آسیب پذیری در حالت جاری (جواب سؤال مثبت باشد) در حالت هدف از بین بردن آن و عدم کاربرد برای آن متصور است. کاربر نرم افزار با تغییر مؤلفه‌های ورودی می‌تواند میزان افزایش سطح امنیت در خروجی را مشاهده و نماید. در واقع با سؤال «چه می‌شود اگر» وضعیت آتی خود را با کم‌ترین هزینه بهبود بخشد.

وضعیت هدف: وضعیت آتی (هدف) در جواب مثبت به سؤالات وضعیت جاری پدید می‌آید که سه حالت دارد:

- ✓ جواب مثبت (در صورت وجود آسیب پذیری) به معنای باقی ماندن آسیب پذیری بعد از امن سازی است.
- ✓ جواب منفی به معنای حذف آسیب پذیری بعد از امن سازی است.
- ✓ جواب Not Applicable (عدم کاربرد) به معنای بی ارتباط نمودن آسیب پذیری بعد از امن سازی است.

این جداول بر اساس وزن دهی اولیه تفکیک شده‌اند اما در این پروژه هر سؤال جدول با هر سه حالت اولیه وزن دهی (محرمانگی ، یکپارچگی و دسترس پذیری) ارتباط دارد. در این جدول ستون هدف وقتی قابل رویت می‌شود که جواب سؤال وضعیت جاری مثبت باشد.

ردیف	سؤالات	current			target			پدافند غیر عامل (امنیت)		
		no	Not apli	yes	no	Not apli	yes	محرمانگی	یکپارچگی	دسترس پذیری

جدول ۸-۲- نمونه خام سطح دوم جداول عملکردی

۸-۱-۳- سطح سوم جداول وضعیت بحران

در پدافند غیر عامل سه وضعیت اقدامات پیش از بحران، حین بحران و پس از بحران باید مشخص گردد. در فضای سایبری قریب به اتفاق اقدامات دیده شده برای جلوگیری از حمله و امن سازی می‌باشد که می‌توان آن‌ها در زمره فعالیت‌های پیش از بحران دسته بندی نمود.

ذکر این نکته ضروری است که در بسیاری از بحران‌های فنی فضای سایبری (مانند حملات) مدت زمان انجام حمله کوتاه بوده و اقدامات شناسایی و جمع آوری اطلاعات در زمان‌های گذشته صورت گرفته است. در نتیجه اقداماتی که باید حین حمله صورت گیرد محدود می‌باشد و در بسیاری از موارد امکانی برای انجام اقدامات متقابل در زمان وقوع حمله وجود ندارد. برای برخی از حملات مانند منع خدمات، شنود اطلاعات، حملات پیمایش درگاه و... اقداماتی در زمان وقوع حوادث قابل تصور است. پس از وقوع حوادث کم اثر کردن آن‌ها و یا خنثی نمودن آن‌ها اهمیت به سزایی دارد. در حملاتی که محرمانگی اطلاعات را مورد هدف قرار می‌دهند اقدامات پس از حادثه معنایی ندارد، در این موارد، دیگر اقدام پس از بحران متصور نمی‌باشد. برای حملاتی که به وب سایت‌ها برای از بین بردن آن‌ها صورت می‌گیرد اقدامات پس از بحران اعم از جایگزینی وب در کوتاه‌ترین زمان ممکن است.

ردیف	سؤالات	تأثیر در وضعیت بحران		
		قبل بحران	حین بحران	بعد بحران

جدول ۸-۳- نمونه خام جدول وضعیت بحران

در این سامانه برای هر آسیب پذیری راه حل مختصری بر اساس مستندات بند ۷ این سند آمده است. برای هر سؤال احتمال وقوع متصور می‌باشد که این مقدار برای هر سؤال به صورت مجزا قابل محاسبه است. در طراحی سامانه احتمال وقوع هر سؤال بین ۰ تا ۱۰۰ درصد در نظر گرفته شده است. و برای ضریب وزنی دلخواه محدوده ای وجود ندارد. آسیب پذیری های مورد پرسش در این سامانه بر اساس نوع آن‌ها و همچنین سه مؤلفه امنیت دسته بندی شده‌اند. برخی از آن‌ها تنها در حوزه محرمانگی و برخی دیگر در حوزه جامعیت و برخی دیگر تنها در حوزه دسترس پذیری تأثیر گذار می‌باشند و ممکن است برخی از تهدیدات متصور در این حوزه در هر سه محور و یا دو محور از سه محور موثر باشند.جدول نهایی پیاده سازی نرم افزار ترکیبی از جداول بالا می‌باشد.

ردیف	گروه آسیب پذیری	نام آسیب پذیری	بند مرتبط	سؤالات	میزان وزن دلخواه	احتمال وقوع	current			target			پدافند غیر عامل (امنیت)		
							no	Not apli	yes	no	Not apli	yes	محرمانگی ایمنی Safety	جامعیت	پایداری دسترس پذیری Stability

جدول ۸-۴- نمونه خام جدول نهایی جهت پیاده سازی سامانه

۸-۲- پدافند غیر عامل در سامانه

به منظور رعایت موارد پدافند غیر عامل در سامانه در دو نقطه مجزا این مبحث مد نظر قرار گرفته شده است. در بخش اول در بین ستون‌های مخفی شده سامانه می‌باشد که در آن‌ها پارامترهای پدافند غیر عامل (ایمنی، امنیت و پایداری) با استفاده از استاندارد ISMS و خلاصه سازی آن‌ها به سه مؤلفه امنیت (محرمانگی، یکپارچگی و دسترس پذیری) در فضای سایبری تطبیق داده شده و در نرم افزار گنجانده شده است.

در بخش دیگر به حوزه‌های موثر در پدافند غیر عامل (استتار، اختفاء، پوشش، فریب، تفرقه، مقاوم سازی و اعلام خبر) که باعث کاهش توان آسیب پذیری می‌شود پرداخته شده است. با استفاده از ابزارهای امن‌ساز می‌توان برای هر یک از حوزه های پدافند غیر عامل، ابزاری را توصیه نمود به عنوان مثال برای فریب می‌توان ابزار کندوی عسل را معرفی نمود. این ابزار وظیفه فریب و انحراف مهاجمین به شبکه را دارد. یکی از سامانه‌هایی که به منظور استتار آدرس‌های اینترنتی[1] مورد استفاده قرار می‌گیرد NAT[2] می‌باشد همچنین جهت اختفا می‌توان از ابزارهایی مانند رمزنگاری و پنهان نگاری استفاده نمود. از روش‌های این حوزه جهت رفع آسیب توصیه

1 - IP Address

2 – Network Address Translation

شده است. جدول زیر نمونه‌ای از توصیه ارائه شده در نرم افزار می‌باشد.

حوزه پدافندی که باعث کاهش توان آسیب پذیری می‌شود.						
استتار	اختفاء	پوشش	فریب	تفرقه	مقاوم سازی	اعلام خبر
-	y	-	y	y	y	y
y	y	-	-	y	y	y

جدول ۸-۵- نمونه پیشنهادات حوزه پدافند غیر عامل برای حذف آسیب

۹- جمع بندی و نتیجه گیری.

ایجاد امنیت فعالیتی هزینه بردار و طولانی مدت است که مستلزم فرهنگ سازی و فراهم آوردن امکانات مورد نیاز این حوزه است؛ لذا باید توازنی برای ارزش اطلاعات در مقابل هزینه و زمان مورد نیاز امنیت برقرار نمود. برای مقابله با هر یک از حملات به شبکه‌های رایانه‌ای راه‌حل‌هایی ارائه شده است لیکن پیاده‌سازی این راه‌حل‌ها هیچ‌گاه تضمین کاملی را ارائه نمی‌کنند و همیشه خطراتی امنیت شبکه‌ها را تهدید می‌نماید. استفاده از ابزارهای امنیتی جهت کاهش ریسک امنیت اطلاعات یکی از الزامات حفظ اطلاعات در این حوزه می‌باشد. اکثر ابزارهای امنیتی به ارائه یک نوع خدمت اجرایی خاص می‌پردازند.

سامانه‌های مدیریت ابزارهایی هستند که مدیران را در جهت نیل به اهدافشان با استخراج اطلاعات و دانش از داده‌های موجود یاری می‌نمایند. وظیفه این سامانه‌ها ارائه اطلاعات دقیق و مربوط در زمان مناسب است. سامانه‌های تصمیم‌یار جهت اجرای مدل‌های پیچیده‌ی آماری و ریاضی، تحلیل داده‌ها و پشتیبانی از تصمیم مورد استفاده قرار می‌گیرند.

به منظور ارزیابی سامانه جامعه آماری از مدیران شبکه در نظر گرفته شده است که پس از استفاده از سامانه به پرسش‌نامه‌ای پاسخ داده‌اند که خلاصه نتایج استخراج شده آن به شرح زیر می‌باشد.

این سامانه به میزان متوسط ۸۴ درصد تهدیدات و ریسک‌های برای شبکه‌های رایانه‌ای را مشخص می‌نماید. ۶۴ مخاطرات و نقاط آسیب پذیر شبکه های رایانه ای را فهرست می‌نماید و به میزان ۸۲ درصد روش‌های نفوذ و حمله را نشان می‌دهد. تا حدود ۷۰ درصد راه حل‌هایی را ارائه می‌نماید که ۷۷ درصد نمودار های آماری آن مفید می‌باشد. تا حدود ۷۰ درصد در تصمیم گیری مفید خواهد بود. سامانه به میزان قریب به ۸۴ درصد مستقل از نوع شبکه بوده و تغییر و بومی سازی آن تا ۸۱ درصد میسر می‌باشد.

با توجه به اینکه وظایف مدیریتی در حوزه فناوری اطلاعات دارای پیچیدگی‌های خاص خود می‌باشند و عوامل موثر بر تصمیم‌گیری در این حوزه گسترده و متفاوت است استفاده از سامانه‌های تصمیم‌یار یکی از بهترین پیشنهادات برای رفع معضلات مدیریتی پدافند غیر عامل می‌باشد. به منظور ایجاد سهولت در تصمیم گیری در موارد ساخت‌نیافته فن‌آوری اطلاعات سامانه تصمیم‌یار با رویکرد "چه خواهد شد اگر" در این مقاله پیشنهاد می‌شود. ابزاری که در این مقاله به آن پرداخته شده است، به صورت مستقیم خدمات امنیتی ارائه نمی‌دهد. این سامانه مدیران امنیت را در اتخاذ تصمیم جهت بهبود امنیت متناسب با نیازها و تهدیدات موجود ضمن تحلیل دارایی‌ها، ابزارهای موجود و خدمات ارائه شده یاری می‌دهد.

مراجع

[۱] اصغر صرافی زاده، علی پناهی، سیستم‌های اطلاعات مدیریت، انتشارات میر، تهران، ۱۳۸۰.

[2] D. J. Power, Decision support systems: concepts and resources for managers, Greenwood Publishing Group, Westport CT, 2002

[3] C. Carlsson, E. Turban, DSS: directions for the next decade, Decision Support Systems, Ludic, London, 2003

[۴] علی امیری، غلامرضا جلالی، جعفر موحدی نیا، جعفر موحدی نیا، مفاهیم نظری و عملی دفاع غیرعامل، انتشارات سپاه پاسداران، تهران، ۱۳۸۵

[۵] جعفر موحدی نیا، اصول و مبانی پدافند غیر عامل، دانشگاه صنعتی مالک اشتر، تهران، ۱۳۸۶

[6] Chairman of the Joint Chiefs of Staff Washington, DC 20318 National Military Strategy to Combat Weapons of Mass Destruction, Washington, DC, 2006

[۷] مهرداد میرعرب، نیم نگاهی به مفهوم امنیت، فصلنامه علوم سیاسی، شماره نهم ,۱۳۸۵ .

[8] BS ISO/IEC 17799 : 2000 Information technology - Code of practice for information security management

[9] C. Brenton, C. Hunt, Mastering network security Edition: 2, John Wiley and Sons, New York, 2002

[10] S. E. Young, D. Aitel, The hacker's handbook: the strategy behind breaking into and defending Networks, CRC press, Kansas City, 2004

[11] S. McClure, S. Shah, S. Shah, Web hacking: attacks and defense, Addison-Wesley, Boston Ma, 2003

[۱۲] ریموند مک‌لئود، سیستم‌های اطلاعات مدیریت، مترجم مهدی جمشیدیان و اکبر مهدی پور، انتشارات دانشگاه اصفهان، ۱۳۷۷.

This page is intentionally left blank