Scientific Journal of
Progress studies: Systems and Strategies
(Autumn 2020, Volume 1, Issue 3: 53 - 96)

Print ISSN: 2717-2872
Online ISSN: 2717-2880

Identifying and Ranking the Factors Influencing The Success of the Integrated Threat Management System

Vahid Bekhradinasab*

Abstract

Firewall is known as one of the most widely used security products in computer network security. During its lifespan, this technology has faced a lot of changes. These changes have occurred mostly due to the emergence of new phenomena in network threats. This research is an attempt to introduce the technologies in the creation of firewalls. Accordingly, this research is intended to identify and prioritize factors affecting the success of the integrated threat management system. This is a mixed research, a combination of quantitative and qualitative reseaerch. Data collection tool in the qualitative section of the research includes semi-structured interviews, and in the quantitative section encompasses a questionnaire. In the qualitative section of the research, the data and information obtained from the interviews were used to identify the factors, and the components and indicators of the factors affecting the success of the integrated threat management system were identified. Furthermore, using Expert Choice and SPSS software, the factors affecting the success of the integrated threat management system were identified and ranked in the quantitative part. In other words, the factors affecting success were identified by the use of Fuzzy Hierarchical Analysis, and the factors affecting success were ranked by the use of Fuzzy TOPSIS method. The statistical population of the study contains the employees of Aminpardazan Kavir Company. This Company contains six smaller companies producing integrated local threat management system approved by the Information Technology Organization. Each company contains 10 specialized managers, senior experts and specialists. The questionnaires were proposed to the employees online. 50 of the 60 managers, senior experts and specialists at the companies responded the questions. The research was conducted in the spring and summer of 2018. The results indicated that individual, functional, organizational, and environmental factors were effective on the success of the integrated threat management system using Fuzzy hierarchical analysis. The ranking of these factors through the Fuzzy TOPSIS method revealed that individual factors occupy the highest ranks, and environmental factors are placed at the lowest ranks.

Keywords: *integrated threat management system, factors affecting success, Fuzzy Hierarchical Analysis, Fuzzy TOPSIS Method.*

---

* PhD in accounting, Islamic Azad University of Najafabad , Iran Vahid.BekhradiNasab@gmail.com

نشریه علمی
پژوهش‌های پیشرفت: سیستم‌ها و راهبردها
(پاییز ۱۳۹۹، سال ۱، شماره ۳: ۹۶ ـ ۵۳)
شاپا چاپی: ۲۸۷۲ ـ ۲۷۱۷
شاپا الکترونیکی: ۲۸۸۰ ـ ۲۷۱۷

شناسایی و رتبه‌بندی عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات

وحید بخردی‌نسب*

تاریخ دریافت: ۱۳۹۹/۰۱/۰۵
تاریخ پذیرش: ۱۳۹۹/۰۹/۱۸

چکیده

فایروال یکی از محصولات امنیتی پرکاربرد در برقراری امنیت شبکه‌های رایانه‌ای است. به‌همین دلیل فناوری فایروال‌ها در طول عمر این محصول تغییرات زیادی داشته است. این تغییرات بیشتر به‌دلیل تولد ایده‌های جدید در تهدیدات شبکه‌ای بوده است. در این پژوهش تلاش شده است فناوری تولید فایروال معرفی شود. بر این اساس هدف این پژوهش شناسایی و رتبه‌بندی عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات است. روش انجام پژوهش آمیخته است. روش آمیخته ترکیبی از روش کمی و روش کیفی است. ابزار گردآوری اطلاعات در بخش کیفی، مصاحبه نیمه‌ساختاریافته و در بخش کمی نیز پرسشنامه است. در بخش کیفی، برای شناسایی عوامل، از داده‌ها و اطلاعات به‌دست‌آمده از مصاحبه استفاده، و مؤلفه‌ها و شاخصهای عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات شناسایی شد. هم‌چنین در بخش کمی، با استفاده از نرم‌افزارهای Expert Choice و SPSS عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات شناسایی و رتبه‌بندی شد. به بیان دیگر شناسایی عوامل مؤثر بر موفقیت با استفاده از تحلیل سلسله‌مراتبی فازی و رتبه‌بندی عوامل مؤثر بر موفقیت با استفاده از شیوه تاپسیس فازی انجام شد. جامعه آماری پژوهش شرکت امن‌پردازان کویر است. شرکت امن‌پردازان کویر شش شرکت تولیدکننده سامانه مدیریت یکپارچه تهدیدات بومی با تأییدیه سازمان فناوری اطلاعات دارد. هر شرکت ۱۰ نیروی متخصص از مدیران، کارشناسان ارشد و کارشناسان متخصص دارد. پرسشنامه‌ها به‌صورت برخط بر روی سامانه شرکت قرار گرفت. از بین ۶۰ نفر مدیران، کارشناسان ارشد و کارشناسان متخصص شرکت امن‌پردازان کویر، ۵۰ نفر پاسخگوی سؤالها بودند. بازه زمانی انجام پژوهش بهار و تابستان ۱۳۹۷ بود. نتایج پژوهش حاکی است که عوامل فردی، عوامل عملکردی، عوامل سازمانی، عوامل محیطی بر موفقیت سامانه مدیریت یکپارچه تهدیدات با استفاده از تحلیل سلسله‌مراتبی فازی مؤثر هستند. رتبه‌بندی هرکدام از این عوامل با استفاده از شیوه تاپسیس فازی به این‌صورت است که عوامل فردی بیشترین نمره و عوامل محیطی کمترین نمره را در رتبه‌بندی به‌خود اختصاص داده است.

کلیدواژه‌ها: *سامانه مدیریت یکپارچه تهدیدات، عوامل مؤثر بر موفقیت، تحلیل سلسله مراتبی فازی، شیوه تاپسیس فازی.*

* دکتری حسابداری، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران vahid.BekhradiNasab@gmail.com

۱. مقدمه

گسترش استفاده از فضای تبادل اطلاعات در کشور طی سالهای گذشته و برقراری ارتباط ازطریق وب، موجب افزایش به‌کارگیری فناوری اطلاعات و وابستگی نهادهای مختلف اجتماعی به این پدیده شده است. از زمانی که درخصوص تعرض به حریم خصوصی افراد و سازمانها برخی نگرانیها ظاهر شد، متخصصان فناوری اطلاعات برای جلوگیری از این تهدیدات و حمایت از اطلاعات خصوصی بنگاه‌ها، افراد و دستگاه‌های مختلف تلاشهای ارزشمندی را ساماندهی کردند تا فضای اعتماد به تبادلات الکترونیکی دچار آسیب کمتری شود. تولید محصولات مختلف امنیتی اعم از تجهیزات سخت‌افزاری و نرم‌افزارها در حوزه‌های گوناگون ICT، ارائه راه‌کارها و تدوین سیاستهای خرد و کلان به‌منظور نگهداری از فضای تبادل اطلاعات، تربیت نیروهای متخصص به‌منظور حفاظت از شبکه‌های تبادل اطلاعات و هم‌چنین ایجاد آمادگی در برابر حوادث ناشی از تهدیدات الکترونیکی، همگام با پیشرفت دانش فناوری اطلاعات در صحنه دنیای دیجیتال رشد بیشتری پیدا کرد. در این میان هم‌زمان با رشد و توسعه انواع آسیب‌پذیری‌ها در سامانه‌های رایانه‌ای، فناوریها در راستای محافظت از این سامانه‌ها نیز ارتقا یافت. رویکرد جدید تهدیدات الکترونیکی عموماً براساس تهدید بر محتوا تلقی می‌شود. این رویکرد بیشتر به‌دلیل حضور تجهیزات امنیتی پایین‌تر از لایه محتوا صورت گرفته است. بدیهی است که امنیت در لایه‌های بالا، مخصوصاً در محتوا بسیار پیچیده است و البته بالاترین سطح امنیت سازمان نیز امنیت در سطح محتوا است. بر این اساس فناوری تجهیزات امنیتی نیز باید به سمت محافظت از تهدیدات محتوایی حرکت کند (مینتزبرگ و وارتز[1]، ۱۹۸۲).

فناوری سامانه مدیریت یکپارچه تهدیدات اخیرترین ایده در تجهیزات امنیتی است که تلاش می‌کند امنیت سازمان را تا سطح محتوا حفظ کند. این فناوری به‌عنوان نسل جدید محصولات فایروال است و پیش‌بینی می‌شود که در آینده نزدیک، محصول سامانه مدیریت یکپارچه تهدیدات به‌عنوان محصول امنیتی ضروری در سازمانها جایگزین فایروال شود. بنابراین با وجود محصولات پیش روی وارداتی و هم‌چنین نمونه‌های کوچک و بزرگ بومی این محصول، بازاری رقابتی پیش روی

1. Mintzberg & Waters

شرکتهای تولیدکننده است. سامانه مدیریت یکپارچه تهدیدات شامل مجموعه‌ای کامل و جامع از تمامی راه‌کارهای امنیت شبکه است. اولین ویرایشهای سامانه مدیریت یکپارچه تهدیدات در اوایل سال ۲۰۰۳ تولید و اولین محصول آن توسط شرکت Serv GATE به بازار ارائه شده است. در ایران نیز محصول سامانه مدیریت یکپارچه تهدیدات از سال ۱۳۹۱ تولید و در حال حاضر نزدیک به ۴۰۰ نمونه آن به بخشهای حاکمیتی و خصوصی عرضه شده است. در این راستا شرکت امن‌پردازان کویر نیز با وجود محصول نوپا و قوی خود برای موفقیت نیازمند شناسایی عوامل موفقیت است.

یکی از ویژگیهای شرکتهای موفق امروز، برخورداری از قدرت رقابت‌پذیری است که بیش از هر چیز، از داشتن دیدگاه‌های جدید در مورد آن نشأت می‌گیرد. در عین‌حال، بستر محیط و زمان، تغییرات چشمگیری در شاخصهای رقابت‌پذیری ایجاد کرده است. باید توجه کرد زمانی چارچوبهای مفهومی رقابت‌پذیری می‌تواند کاربرد دائمی داشته باشد که به‌قدر کافی برای سازگاری فرایندهای مدیریتی و تغییرات محیطی انعطاف‌پذیر باشد (امباشتا و مومایا[1]، ۲۰۰۲). امروزه برقراری امنیت، ایمنی و پایداری شبکه، برای ادارات و شرکتهای دولتی و سازمانهای کوچک و بزرگ مسئله‌ای مهم است. تهدیدهای پیشرفته ازسوی تروریست‌های فضای سایبر، کارمندان ناراضی و هکرها، رویکردی سامانمند را برای برقراری امنیت، ایمنی و پایداری شبکه می‌طلبد. در بسیاری از صنایع، امنیت یک انتخاب نیست بلکه یک ضرورت است. در این میان بخش قابل‌توجهی از بار فنی و مسئولیتی برقراری امنیت، ایمنی و پایداری بر عهده کارشناسان امنیت شبکه سازمانها و شرکتها است (برونو و تابیجی[2]، ۱۹۸۲). این کارشناسان باید با پیاده‌سازی مکانیزه‌ها و استفاده از تجهیزات امنیتی مختلف موجبات برقراری امنیت، ایمنی و پایداری در داده‌های سازمان مطبوع را فراهم کنند. در بیشتر موارد کارشناسان امنیت شبکه با مشکلات زیادی در دستگاه‌های امنیتی ازجمله عدم سازگاری دستگاه‌ها با یکدیگر و عدم وجود دستگاهی برای تحلیل گزارشهای تولیدشده توسط تجهیزات مختلف روبه‌رو هستند. از این‌رو شرکتهای سازنده تجهیزات امنیتی به فکر مجتمع‌کردن دستگاه‌های موازی و حذف وظایف موازی آنها هستند که نتیجه کار این شرکتها عرضه محصول «سامانه مدیریت تهدید یکپارچه» است. به

1. Ambashta and Momaya
2. Bruno & Tyebjee

هر حال هر سازمانی برای ایجاد ارتباط بهتر با گروه‌های مخاطب و مشتریان خود تدابیری اندیشیده است. اینترنت یکی از مناسبترین و در عین حال ساده‌ترین راه‌های ایجاد ارتباط دوسویه است. سازمانهای بزرگ و کوچک نیازمند ایجاد سیاستهای امنیتی لازم درخصوص استفاده از رایانه و ایمن-سازی اطلاعات و شبکه‌های رایانه‌ای هستند. سیاستهای امنیتی، مجموعه قوانین لازم به‌منظور استفاده از رایانه و شبکه‌های رایانه‌ای بوده که در آن وظایف تمام کاربران دقیقاً مشخص و درصورت ضرورت، هشدارهای لازم به کاربران درخصوص استفاده از منابع موجود در شبکه داده می‌شود. برای امن‌سازی ارتباطات درون‌سازمانی، میان‌سازمانی و اینترنتی هر سازمان، نیاز به استفاده از سرویس‌های امنیتی متعدد در شبکه و مخصوصاً در دروازه آن می‌باشد که یکی از راه‌کارهای امنیتی، محافظت با دیواره آتش است (مک‌کللند[1]، ۱۹۸۷). دیواره آتش سامانه یا ترکیبی از سامانه‌ها است که از یک سیاست کنترل دسترسی بین دو شبکه حمایت می‌کند. هم‌چنین ممکن است برای توصیف نرم‌افزاری که از منابع رایانه‌ای حمایت می‌کند یا ترکیبی از نرم‌افزار، سخت‌افزار و سیاستهایی (نرم‌افزار دیواره آتش) که از این منابع حفاظت می‌کنند، اصطلاح دیواره آتش استفاده شود. رایجترین محل برای دیواره آتش بین شبکه‌های داخلی سازمان و اینترنت است، که دیواره آتش یکی از مزایای سامانه مدیریت تهدید یکپارچه است (کرمی، ۱۳۹۲). از این‌رو، کشورهای مختلف به تولید سیستم عامل سامانه مدیریت تهدید یکپارچه فکر کرده‌اند و شرکتهایی مثل سفوس، سیسکو و جونیپر در این عرصه فعالیت دارند و در سال‌های اخیر شرکت‌های ایرانی نیز دست به تولید این محصول زده‌اند و با مشکلات رقابتی در این بازار روبرو هستند. استفاده از دستگاه‌های امن‌سازی نظیر دیواره آتش، سامانه تشخیص و پیشگیری از نفوذ و ویروس‌یاب به‌صورت مجزا به‌دلایل زیر توصیه نمی‌شود:

۱. به ازای هر یک از سرویس‌ها، هزینه خرید سخت‌افزار و یا نرم‌افزار باید مجزا پرداخت شود. مدیر شبکه باید به چگونگی کارکرد چندین دستگاه یا سرویس آشنا باشد.

۲. از آنجاکه معمولاً چینش دستگاه‌ها و سرورها به‌طور سری پشت سر هم هستند، هر یک از دستگاه‌ها به‌عنوان گلوگاه محسوب شده و کندی یا قطعی در هر دستگاه، کار دستگاه‌های دیگر را

1. Mcclelland

مختل می‌کند.

۳. در هر یک از دستگاه‌ها، بسته‌های اطلاعاتی یک‌بار گشوده شده، چک می‌شود و دیگر بار بسته می‌شود. بنابراین تأخیر زیادی از زمان ارسال بسته تا دریافت بسته در مقصد نهایی ایجاد می‌شود.

۴. در برخی موارد به‌دلیل عدم سازگاری امکانات امنیتی دستگاه‌های مجزا، از این امکانات در کنار یکدیگر برای امن‌سازی شبکه نمی‌توان بهره جست.

به‌عنوان‌مثال درصورتی‌که برای امن‌سازی برخی سرویسها در محیط اینترنت از سرویس IPSec VPN استفاده شود، دیواره آتش و سایر دستگاه‌ها امکان بررسی بسته‌های عبوری را نخواهند داشت. درصورتی‌که اگر بتوان از دیواره آتش موجود در دروازه به‌عنوان VPNServer نیز استفاده کرد، با رمزگشایی بسته‌های اطلاعاتی در دیواره آتش امکان بررسی این بسته‌ها نیز وجود خواهد داشت.

امروزه توجه به خطر در مهندسی سازمان از زمان افزایش فضای کسب و کار رقابتی‌تر، پیچیده و غیرقابل پیش‌بینی است (لامین و همکاران[1]، ۲۰۲۰). در سال‌های اخیر، برای رفع مشکلات فوق در دروازه، دستگاه‌هایی عرضه شده‌اند که بیشتر یا همه نیازهای امنیتی در دروازه را به‌صورت راه‌حل امنیتی جامع و واحد ارائه می‌دهند. از این دستگاه‌ها با عنوان سامانه مدیریت تهدید یکپارچه یاد می‌شود. ازجمله مشکلات پیش‌گفته، عدم رقابت‌پذیری است که یکی از ارکان این مشکل بزرگ عدم شفافیت بازار است. منظور اینکه اطلاعات به‌اندازه کافی در محیط بازار وجود ندارد. بنابراین معاملات و مبادلات با کارایی زیاد انجام نمی‌شود. در صورتی‌که اطلاعات موجود در بازار افزایش یابد، از یک طرف مشتریان خریدهای بهینه را انجام خواهند داد و از طرف دیگر تولیدکنندگان نیز ترغیب می‌شوند که برای حفظ یا افزایش سهم بازار خود تلاش بیشتری کنند (صارمی، ۱۳۸۵). بنگاه‌ها به‌منظور کسب مزیت رقابتی پایدار، باید مشتری‌گرا یا بازارگرا، نوآور و کارآفرین و نیز گرایش زیادی به یادگیری داشته باشند. بر اساس این دیدگاه، گرایش به بازار، منبعی مهم برای به‌دست‌آوردن مزیت رقابتی و حتی مزیت رقابتی پایدار به‌حساب می‌آید (لیو و همکاران[2]، ۲۰۰۳). در این رویکرد، ساختار صنعت، عاملی مؤثر بر کسب توان رقابتی آن به‌شمار می‌رود. این ساختار، ارزش

1. Lamine et al.
2. Liu et al.

ایجادشده توسط فعالیتهای اقتصادی اعضای صنعت و نیز توان آنها برای سهیم‌شدن در ثروت ایجادشده را توصیف می‌کند (هاکس و وایلد[1]، ۱۹۹۹: ۲۰۰۲). این رویکرد با استفاده از چارچوبهایی مانند ساختار صنعت، زنجیره ارزش و راهبردهای عمومی، پایه و اساس تعیین مزیت رقابتی و طراحی راهبردهای خارج از سازمان است (حق‌شناس، ۱۳۹۰). منابع مبتنی بر بازار نیز که از تنوع زیادی برخوردارند عبارت است از: قابلیتهای ارتباط با مشتری، داراییهای مبتنی بر شهرت، منابع انسانی و توان نوآوری موفقیت‌آمیز در بازار (هولی و همکاران[2]، ۲۰۰۳). ارزیابی عملکرد بنگاه‌ها ازجمله مباحث مدیریت است که قابل بحث و بررسی است. هم‌چنین به تجربه ثابت شده در شرایط رقابتی مؤسساتی باقی می‌مانند که قوی و نیرومند بوده و به شکل کارا و مؤثر فعالیت کنند (بازایی، ۱۳۹۱). بنابراین مسئله این است که با توجه به شرایط خاص صنعت در دهه اخیر کدام عوامل است که شرکتها با دستیابی به آنها می‌توانند از رقیبان خود پیشی گرفته و سود خود را افزایش دهند (مظلومی، ۱۳۹۱). در راستای پاسخ به سؤال بیان شده، در این پژوهش سعی بر آن است که با استفاده از منطق فازی، عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات شناسایی شود تا شرکتهای ایرانی بتوانند با این سامانه نوپا از رقیبان خود سبقت بگیرند. مینیگ و همکاران[3] (۲۰۱۹) معتقدند عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات برای شرکت هرچه سریعتر شناسایی شود، شناسایی و رفع آسیب‌پذیریهای امنیتی مقرون به صرفه‌تر است و بنابراین احتمال وقوع خطر را کاهش می‌دهد. به هر صورت این پژوهش مبتنی بر توان خلاقیت و نوآوری است که در برگیرنده توان تحقیق و توسعه، تـوان به‌کارگیری فناوری اطلاعات و مدیریت دانش است (مک گاهان و سیلورمن[4]، ۲۰۰۶؛ ۱۹۹۹). این پژوهش در نظر دارد با شناسایی و رتبه‌بندی عوامل مؤثر بر موفقیت با کاهش خطر به ارتقای محصول و موفقیت تولید بومی در سطح ملی و بعضاً بین‌المللی کمک کند و ازآنجا که در استان یزد، واحد امنیت اطلاعات شرکت امن‌پردازان کویر در راستای تولید ملی به طراحی، تولید و پیاده‌سازی سامانه مدیریت یکپارچه تهدیدات اقدام و پس از آزمایش محصول و ارزیابی سازمان فناوری

1. Hax & Wilde
2. Hooley et al.
3. Meinig et al.
4. McGahan & Silverman

اطلاعات ایران، با نام تجاری APK GATE روانه بازار کرده، مورد مطالعه این محصول انتخاب شده است. باتوجه به مطالب بیان‌شده این پژوهش به‌دنبال پاسخ به این سؤال است که چه عواملی بر موفقیت سامانه مدیریت یکپارچه تهدیدات در شرکت امن‌پرداز کویر تأثیرگذارند و هرکدام از عوامل از چه رتبه‌ای برخوردار است.

۲. مبانی نظری و پیشینه پژوهش

تهدیدات و نقض پایگاه داده‌ها، نقض حریم خصوصی و حملات سایبری به شرکتها و سازمانهای دولتی مشکلات رو به رشدی را برای شرکتها به‌همراه دارد (مینیگ و همکاران، ۲۰۱۹). نیاز به راه‌حلهای سامانه مدیریت یکپارچه تهدیدات باتوجه به تعداد فزاینده حملات از قبیل هک و شکستن، ویروسها و کرم‌ها بر روی سامانه‌های اطلاعاتی شرکتها ظهور کرد که اکثراً حاصل ترکیبی از تهدیدات خارجی و یا تهدیدات خودی است. در جدیدترین روشهای حمله، کاربر به‌عنوان ضعیف‌ترین حلقه در یک بنگاه اقتصادی هدف قرار می‌گیرد که پیامدهای آن به‌مراتب جدی‌تر از تصور است. به‌عنوان مثال به نقل از دفتر امنیت اطلاعات فدرال[1] (۲۰۱۸)، مرکز جهانی امنیت سایبر در حاشیه مجمع جهانی اقتصاد ضرر سالانه ۴۴۵ میلیارد دلار به دلیل حملات سایبری به نهادهای مالی را تأیید کرده است. هم‌چنین انجمن مشاوران اقتصادی کاخ سفید در گزارش گاردین[2] (۲۰۱۸) مدعی شد که فعالیتهای خرابکارانه سایبری در سال ۲۰۱۶ بین ۵۷ تا ۱۰۹ میلیارد دلار به اقتصاد امریکا ضربه زده است. امنیت داده‌ها و دسترسی‌های غیر مجاز کارمندان به نگرانی اصلی برای تجارت سازمانها تبدیل شده است. به این دلیل که اهداف مخرب و در نتیجه از دست دادن اطلاعات محرمانه می‌تواند به زیانهای عظیم مالی و هم‌چنین به بدهیهای قانونی منجر شود. شرکتها امروزه آغاز به تصدیق این واقعیت کرده‌اند که جهل کاربر می‌تواند باعث به‌خطرافتادن امنیت حیاتی شبکه‌های داخلی شود. مزیتهای اصلی استفاده از راه‌حلهای یو. تی. ام.، سادگی نصب، استفاده کارامد و توانایی به‌روزرسانی همه توابع امنیتی به‌طور هم‌زمان است. بنابراین، علاوه‌بر یک خرید مقرون‌به‌صرفه، هزینه‌های فعالسازی

1. Federal Office for Information Security
2. Guardian

در شبکه روزبه‌روز به شکل قابل توجهی از راه‌حلهای دیگر پایینتر خواهد شد. هدف نهایی سامانه مدیریت یکپارچه تهدیدات ارائه مجموعه‌ای جامع از ویژگیهای امنیتی در محصول واحد مدیریت‌شده از طریق کنسول واحد است. راه‌حلهای یکپارچه امنیتی به‌عنوان یک راه منطقی برای مقابله با تهدیدات فزاینده اینترنتی که به‌صورت پیچیده‌ای باهم ترکیب می‌شدند و سازمانها را تحت تأثیر قرار می‌دادند، تکامل یافتند. بازار سامانه مدیریت یکپارچه تهدیدات با افزایش ۲۰/۱٪ در سال ۲۰۰۹ به‌دنبال افزایش ۳۲/۲٪ در سال ۲۰۰۸ رشد چشمگیری از خود نشان داده است.

گسترش استفاده از فضای تبادل اطلاعات در کشور طی سالهای گذشته و برقراری ارتباط از طریق وب، موجب افزایش به‌کارگیری فناوری اطلاعات و وابستگی نهادهای مختلف اجتماعی به این پدیده شده است. از زمانی که برخی از نگرانیها درخصوص تعرض به حریم خصوصی افراد و سازمانها ظاهر شد، متخصصان فناوری اطلاعات برای جلوگیری از این تهدیدات و حمایت از اطلاعات خصوصی بنگاه‌ها، افراد و دستگاه‌های مختلف تلاشهای ارزشمندی را ساماندهی کردند تا فضای اعتماد به تبادلات الکترونیکی دچار آسیب کمتری شود. تولید محصولات مختلف امنیتی اعم از تجهیزات سخت‌افزاری و نرم‌افزارها در حوزه‌های گوناگون ICT، ارائه راه‌کارها و تدوین سیاستهای خرد و کلان به‌منظور صیانت از فضای تبادل اطلاعات، تربیت نیروهای متخصص به‌منظور حفاظت از شبکه‌های تبادل اطلاعات، هم‌چنین ایجاد آمادگی در برابر حوادث ناشی از تهدیدات الکترونیکی، همگام با پیشرفت دانش فناوری اطلاعات در صحنه دنیای دیجیتال نمود بیشتری پیدا کردند. در این میان هم‌زمان با رشد و توسعه انواع آسیب‌پذیریها در سامانه‌های رایانه‌ای، فناوری در راستای محافظت از این سامانه‌ها نیز ارتقاء یافته‌اند. رویکرد جدید تهدیدات الکترونیکی عموماً بر اساس تهدید بر محتوا تلقی می‌شود. این رویکرد بیشتر به‌دلیل حضور تجهیزات امنیتی پایین‌تر از لایه محتوا صورت گرفته است. بدیهی است که امنیت در لایه‌های بالا، مخصوصاً در محتوا بسیار پیچیده است و البته بالاترین سطح امنیت سازمان نیز امنیت در سطح محتوا است. بر این اساس فناوری تجهیزات امنیتی نیز باید به سمت محافظت از تهدیدات محتوایی حرکت کند. فناوری سامانه مدیریت یکپارچه تهدیدات فکر جدیدتری در تجهیزات امنیتی است که تلاش می‌کند امنیت سازمان را تا سطح محتوا حفظ کند. این

فناوری به‌عنوان نسل جدید از محصولات فایروال است و پیش‌بینی می‌شود که در آینده نزدیک، محصول سامانه مدیریت یکپارچه تهدیدات به‌عنوان محصول امنیتی ضروری در سازمانها جایگزین فایروال شود. در این راستا در چارچوب نظری پژوهش به ادبیات موضوعی تعریف مدیریت تهدید یکپارچه، امن‌سازی شبکه توسط یو. تی. ام.، فناوری فایروال و نیازمندیهای جدید، تعریف سامانه مدیریت یکپارچه تهدیدات، محصول سامانه مدیریت یکپارچه تهدیدات، معماری محصول، مزایای سامانه مدیریت یکپارچه تهدیدات، چالشهای تولید محصول و پژوهشهای مرتبط با موضوع پژوهش پرداخته شده است.

سامانه مدیریت یکپارچه تهدیدات

نام سامانه مدیریت یکپارچه تهدیدات[1] یا مدیریت یکپارچه تهدیدات الکترونیکی عبارتی است که برای اولین‌بار توسط شرکت IDC در سال ۲۰۰۴ ابداع شد. محصول سامانه مدیریت یکپارچه تهدیدات راه حل جامع امنیتی است که مسئول محافظت سامانه در برابر چندین نوع تهدید است. محصول سامانه مدیریت یکپارچه تهدیدات معمولاً شامل فایروال، VPN، نرم‌افزار آنتی‌ویروس، فیلترینگ محتوا، فیلتر اسپم، سامانه‌های جلوگیری و تشخیص حمله (IPS) ، حفاظت از Spyware ها و نظارت، گزارشگیری و مدیریت یکپارچه است. از سامانه مدیریت یکپارچه تهدیدات می‌توان به‌عنوان نسل تحول‌یافته محصولات Firewall/VPN و حتی دروازه‌های امنیتی نام برد که سعی در ارائه سرویس‌های امنیتی به کاربران سازمان به ساده‌ترین شکل دارد. درواقع بدون وجود سامانه مدیریت یکپارچه تهدیدات و در راه حلهای قدیمی برای به‌دست‌آوردن تک‌تک این سرویسهای امنیتی ابزارهای مجزا به‌همراه پیچیدگیهای نصب، به‌روزسازی و مدیریت آنها نیاز بود. اما سامانه مدیریت یکپارچه تهدیدات با یکپارچه‌سازی و مدیریت متمرکز، تمام نیازمندیهای امنیتی سازمان در برابر تهدیدات الکترونیکی را برآورده می‌سازد (انیسا[2]، ۲۰۱۸).

مدیریت تهدید یکپارچه

مدیریت تهدید یکپارچه راه حل جامعی است که به‌تازگی در صنعت امنیت شبکه پدید آمده

1. Unified Threat Management
2. Enisa

است و از سال ۲۰۰۴ صرفه‌جویی گسترده‌ای را به‌عنوان راه‌حل شاهراه دفاعی شبکه‌های اصلی برای سازمانها به‌دست آورده است. در تئوری، سامانه مدیریت یکپارچه تهدیدات، تکامل دیواره‌های آتش (فایروال‌های) سنتی به یک محصول امنیتی فراگیر است که قادر به انجام وظایف امنیتی متعدد در داخل یک دستگاه است. دیواره آتش شبکه، جلوگیری از نفوذ شبکه و دروازه ضد ویروس، ای. وی. (AV) و دروازه ضد هرزنامه، وی. پی. ان.، فیلترینگ محتوا، حفظ تعادل بار، پیشگیری نشست اطلاعات روی گزارش دستگاه است. بازار جهانی سامانه مدیریت یکپارچه تهدیدات تقریباً به ارزش ۲/۱ میلیارد دلار در سال ۲۰۰۷ بود و با پیش‌بینی ۳۵ ـ ۴۰٪ نرخ رشد مرکب سالانه تا سال ۲۰۱۱ است. بازار اصلی ارائه‌دهندگان سامانه مدیریت یکپارچه تهدیدات، smb و بخش سازمانی است؛ اگرچه در حال حاضر ارائه‌دهندگان کمی در حال ارائه راه‌حلهای سامانه مدیریت یکپارچه تهدیدات برای دفاتر کوچک یا ادارات از راه دور هستند. اصطلاح سامانه مدیریت یکپارچه تهدیدات در اصل توسط شرکت تحقیقاتی بازار IDC ابداع شد. مزایای استفاده از وضعیت امنیتی یکپارچه در این واقعیت است که به‌جای مدیریت سامانه‌های مختلف که به‌صورت جداگانه آنتی‌ویروس‌ها، فیلترینگ محتوا، جلوگیری از نفوذ و توابع فیلترینگ اسپم‌ها را اداره می‌کنند، سازمان در حال حاضر انعطاف‌پذیری لازم برای استقرار یک دستگاه یو. تی. ام. را دارد که تمام قابلیتهای خود را در یک چارچوب از ابزار و وسایل شبکه نصب‌شدنی قرار دهد.

امن‌سازی شبکه توسط سامانه مدیریت یکپارچه تهدیدات

دستگاه سامانه مدیریت یکپارچه تهدیدات ساده مدیریت راهبرد امنیتی یک شرکت را آسان‌تر می‌کند. فقط با یک دستگاه می‌توان محل لایه‌های مختلف سخت‌افزار و نرم‌افزار را در نظر گرفت. هم‌چنین به‌وسیله یک کنسول متمرکز، تمام راه‌کارهای امنیتی می‌تواند تحت نظارت و پیکربندی باشد. در این زمینه، سامانه مدیریت یکپارچه تهدیدات شکل واحدی از وسایل امنیتی را نشان می‌دهد که انواع قابلیتهای امنیتی ازجمله دیواره آتش، وی. پی. ان. (VPN)، دروازه‌های ضد ویروس، ضد هرزنامه دروازه، جلوگیری از نفوذ، فیلترینگ محتوا، مدیریت پهنای باند، نرم‌افزار کنترل و گزارشدهی متمرکز را به‌عنوان ویژگیهای اساسی در بر دارد. سامانه مدیریت یکپارچه تهدیدات، برای

نگه‌داشتن تمام ویژگیهای امنیتی در یک مکان سیستم عامل سفارشی دارد که می‌تواند به ادغام بهتر مجموعه‌ای از دستگاه‌های نامتجانس منجر شود. برای شرکتهای با شبکه از راه دور یا ادارات واقع‌شده در فاصله دورتر، سامانه مدیریت یکپارچه تهدیدات وسیله‌ای است برای تأمین امنیت متمرکز با کنترل کامل بر شبکه‌هایی که در جهان توزیع شده‌اند.

فناوری فایروال و نیازمندیهای جدید

فناوری فایروال و نیازمندیهای جدید شامل تهدیدات محتمل سامانه‌های رایانه‌ای و نقش ابزارهای کنترل ترافیک است، که در قسمت بعد هر کدام تشریح شده است.

۱. تهدیدات محتمل سامانه‌های رایانه‌ای

به‌منظور مقابله با تهدیداتی که حوزه‌های مختلف فناوری اطلاعات ممکن است با آن روبه‌رو باشد، شناخت نوع تهدید ضروری است. بدیهی است سامانه یکپارچه مقابله با تهدیدات باید به‌صورت مشخص انواع موردنظر را پوشش داده و راه‌کارهای پیشنهادی را ارائه کند. انواع حملات و تهدیدات را می‌توان به‌صورت حملات تخریب سرویس، حمله از طریق برنامه مخرب و حمله انسانی و فیزیکی دسته‌بندی کرد. در هر یک از دسته حملات، فعالیتهای متفاوتی ازسوی مهاجمین قابل اجرا است. در این بخش فهرستی از این فعالیتها بیان می‌شوند.

حملات تخریب سرویس: در این نوع حمله، مهاجم تلاش می‌کند تا دسترسی منابع رایانه توسط سایر کاربران را ناممکن سازد. برای دستیابی به این هدف، چنانچه منابع مشترک سامانه به‌گونه‌ای توسط مهاجم اشغال شده و حجم استفاده از آنها افزایش یابد که دیگران به استفاده از آنها قادر نباشند، عملاً حمله به منابع سامانه صورت گرفته است. این نوع حمله می‌تواند به تخریب منابع منجر شود و یا استفاده از آنها را غیرممکن سازد. برخی از فعالیتهای این نوع تهدید تخریب، پرکردن و حذف فایلهای اساسی دیسک، تولید پردازش و اشغال پهنای باند پردازنده، تخریب و کنترل سرویسهای شبکه توسط مهاجم، ذخیره پیام‌های پخش‌شده، ارسال پیام و درخواست پاسخ از رایانه‌های شبکه و استفاده از اتصال‌های غیر باز است.

حمله از طریق برنامه مخرب: در این نوع حمله، برنامه‌ها به‌گونه‌ای نوشته می‌شود که رفتاری

مخرب و غیر عادی داشته باشد. معمولاً این برنامه‌ها از طرق مختلف برای کاربران رایانه ارسال شده و کاربر بدون توجه به وجود دستورالعمل مخرب نسبت به اجرای آن اقدام می‌کند. شیوه‌های مختلف تخریب این برنامه‌ها شامل حمله به برنامه‌های سرویس‌دهنده شبکه، تخریب نرم‌افزارها از طریق ارسال پست الکترونیکی، ارسال هرزنامه‌ها، استفاده از درب‌های مخفی برای دسترسی غیرمجاز و اسب‌های تراوا و کرم است.

حمله انسانی و فیزیکی: چنانچه بر اساس ضعف‌های موجود در برخی از سامانه‌ها، نفوذگر بتواند به‌عنوان راهبر سامانه شناخته شود، با در دست‌گرفتن کنترل سامانه می‌تواند صدماتی را وارد کند. به‌علاوه هر مهاجمی می‌تواند به‌صورت فیزیکی منابع سامانه را مورد حمله قرار داده و کارکرد آن را دچار مشکل سازد. فعالیتهای سرقت رمز عبور، نفوذ از طریق برقراری روابط اجتماعی و تخریب فیزیکی منابع رایانه‌ای و شبکه‌ای توسط مهاجم قابل انجام است.

۲. نقش ابزارهای کنترل ترافیک

امروزه فایروال‌های حالت‌مند[1]، IDS ها و آنتی‌ویروس‌های مبتنی بر میزبان[2] محبوب‌ترین محصولات امنیتی هستند. اما این راه‌حل‌ها به‌سرعت در حال از دست دادن تأثیر خود در برابر نسل جدید تهدیدات هستند و متخصصان فناوری اطلاعات حملات و سرایت‌های موفق متعددی را بر ضد امنیت و زیرساخت شبکه مشاهده می‌کنند.

نقش سامانه‌های فایروال سنتی و کمبودهای آنها

فایروال‌های حالت‌مند در ابتدا برای امن‌سازی ارتباط با اینترنت به‌وسیله یک واسط امن بین شبکه‌های قابل اعتماد و غیرقابل اعتماد طراحی شد. این فایروال‌ها با دقت در سرآیند لایه شبکه (L3) و لایه پروتکل (L4) بسته را نظارت کرده و بر اساس آن به ترافیک اجازه ورود داده، درخواست ورود آن را رد کرده و یا ترافیک را دوباره بر اساس مجموعه‌ای از خط‌مشی‌های فایروال مسیریابی می‌کند. مشکل اصلی فایروال‌ها در این است که هکرها روشهای متعددی را برای گذشتن از خط‌مشی‌های فایروال توسعه داده‌اند. بعضی از این روشها عبارت است از: پویش پورت‌های باز روی

1. Stateful
2. Host Based Antivirus

فایروال و یا سامانه‌های موجود در ناحیه قابل اعتماد، نرم‌افزارهای مخرب نظیر نروژان‌هایی که روی سامانه‌های موجود در ناحیه قابل اعتماد نصب شده‌اند و می‌توانند به‌عنوان شروع‌کننده حملات نقش داشته باشند، عدم توانایی فایروال‌های نسل قدیمی در بازرسی بخش داده‌های بسته به‌منظور شناسایی انواع شناسه‌های مخرب نظیر ویروس، کرم و یا تروژان، که می‌تواند به‌عنوان مسیر قابل نفوذ برای حمله مورد استفاده قرار گیرد. بسیاری از فایروال‌های جدید که قابلیت بازرسی عمیق[1] را پشتیبانی می‌کنند، در مقابل بسته‌های تکه‌تکه شده آسیب‌پذیر هستند. کاربران با استفاده از سامانه‌های قابل حمل نظیر Laptop و یا PDA، می‌توانند حامل انواع شناسه‌های مخرب و آلوده از بیرون به داخل سازمان شوند. درنتیجه باید اذعان کرد فایروال‌هایی که ما را احاطه کرده‌اند در جهت ممانعت از حملات و سرایت‌هایی که از داخل شبکه قابل اعتماد آغاز شده باشند، کمکی نمی‌کنند.

نقش سامانه‌های IDS سنتی و کمبودهای آنها

همانند فایروال‌های سنتی، IDSهای سنتی با آمدن تهدیدات مدرن و پیچیده جای خود را به فناوریهای جدیدتر می‌دهند. حمله‌کنندگان ضعف‌های سامانه‌های IDS را شناخته و برای گذشتن از این سامانه‌های نظارتی روشهای جدیدی را اجرا کرده‌اند. مثال‌هایی از ضعف سامانه‌های IDS عبارت است از: محصولات IDS معمولاً در نقاط لب‌های شبکه مستقر می‌شوند و نظارتی بر کل شبکه ندارند، سامانه‌های IDS معمولاً به‌عنوان ابزارهای نظارتی کاربری دارند و قابلیت ممانعت از ترافیک مشکوک در این سامانه‌ها وجود ندارد، به‌دلیل چگونگی بازرسی در سامانه‌های IDS، این سامانه‌ها معمولاً در مقابل حجم زیاد ترافیک آسیب‌پذیر می‌شوند، اغلب سامانه‌های IDS حجم زیادی false positive تولید می‌کنند که برای جلوگیری از این امر به نظارت مداوم بر کار IDS نیاز است، برای حل مشکلات فوق، بسیاری از تولیدکنندگان محصولات IDS، به سمت تولید نسل جدیدی از این محصولات به نام IPS روی آورده‌اند. سامانه‌های IPS می‌تواند به‌صورت Inline در توپولوژی شبکه قرار گیرند و کنش‌های مورد نیاز مدیر نظیر Drop و یا Reset را اعمال کنند. این محصولات هم‌چنین می‌توانند از ساختارهای تشخیص Anomaly بهره‌مند شوند.

1. Deep Inspection

آنتی‌ویروس‌های مبتنی بر میزبان و کمبودهای آنها

یکی از پرکاربردترین نرم‌افزارهای امنیتی، سامانه‌های آنتی‌ویروس مبتنی بر میزبان است. این نرم‌افزارهای آنتی‌ویروس به‌عنوان یکی از معمول‌ترین راه‌حل‌های امنیتی در سازمانها استفاده می‌شود. قدمت استفاده از این نرم‌افزارها از سال ۱۹۸۰ میلادی و به‌دلیل حضور فایل‌های ویروسی است. گرچه حضور نرم‌افزارهای آنتی‌ویروس مبتنی بر میزبان در سازمانها یک ضرورت تلقی می‌شود. ولی این راه‌حل‌ها شامل نقاط ضعف نیز هستند. نقاط ضعف‌ها عبارت است از: پیچیدگی فرایند نصب، غیرفعال‌سازی عمدی و یا غیر عمدی آنتی‌ویروس توسط کاربران، آسیب‌پذیری نرم‌افزار آنتی‌ویروس در مقابل به‌روزرسانی‌ها. فرایند نصب، نگهداری و ارتقای الگوهای ویروسی برای این نرم‌افزارها پیچیده است. باید توجه داشت که این نرم‌افزارها باید در تمامی میزبان‌های سازمان نصب شود. کاربران به‌صورت عمدی و یا غیر عمدی می‌توانند آنتی‌ویروس خود را غیر فعال کنند. اغلب کاربران فرایندی منظم برای به‌روزرسانی الگوهای ویروس برای نرم‌افزار آنتی‌ویروس خود اتخاذ نمی‌کنند و معمولاً در مقابل اخیرترین نسخه ویروس‌ها آسیب‌پذیر هستند. برخی از تروژان‌های پیشرفته قادرند قبل از فعال‌شدن آنتی‌ویروس روی میزبان فعال شوند و هم‌چنین از فعال‌شدن آنتی‌ویروس نیز جلوگیری می‌کنند. بدیهی است سازمانهایی که از نرم‌افزارهای آنتی‌ویروس مبتنی بر میزبان استفاده می‌کنند، در زمینه امنیت سیستم عامل میزبان و برنامه کاربردی از سطح امنیتی خوبی برخوردارند. ولی باید توجه داشت که این سطح امنیتی برای سازمان کافی نیست. به‌طور خاص باید توجه داشت که بسیاری از شناسه‌های مخرب از ناحیه غیر قابل اعتماد وارد نواحی قابل اعتماد شبکه می‌شوند؛ بنابراین سازمان باید بتواند این شناسه‌های مخرب را قبل از رسیدن به میزبان‌ها تشخیص داده و بلاک کنند.

نیاز به محصول U

نیاز به محصول U ریشه در روشهای سنتی و کهن و روشهای نوین دارد که این دو روش به‌شرح ذیل است:

روشهای سنتی (امنیت لایه‌ای به‌صورت چندنقطه‌ای)

امروزه بسیاری از سازمانها سعی در پیاده‌سازی سامانه‌های امنیتی با ترکیب راه‌حل‌های مختلف از

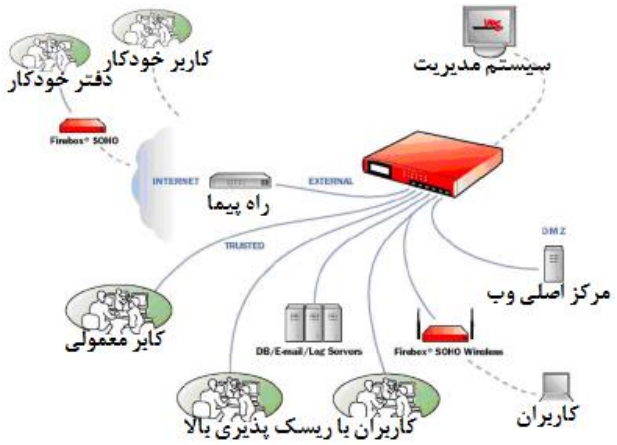
فروشندگان متفاوت دارند. همگی این محصولات باید به‌صورت مجزا خریداری، نصب، مدیریت و به‌روزرسانی شود. این رویکرد مشکلاتی شامل تعامل و همکاری نامناسب بین سامانه‌های امنیتی مجزا، حفاظت ناکامل و آزمون و دستیابی زمان‌بر دارد که همگی باعث کاهش پاسخ شبکه به حملات می‌شوند. محصولاتی که برای کار با هم طراحی نشده باشند، می‌توانند در نرخ کارایی شبکه تأثیر بگذارند. هم‌چنین هزینه لازم برای تهیه انواع محصولات مختلف امنیتی برای رسیدن به امنیت جامع در هر سازمان کوچک یا متوسط بسیار سنگین است. سازمانها به‌ندرت دارای زیرساخت فناوری اطلاعات لازم برای نگهداری و مدیریت چنین مخلوطی از محصولات متفاوت هستند که هرکدام دارای سامانه مدیریت خاص خود می‌باشند؛ و درنهایت هزینه نگهداری و پشتیبانی از رویکردهای چندنقطه‌ای برای سازمانی کوچک یا متوسط بسیار زیاد است. به دلیل این مشکلات، پیچیدگیها و ضعف‌ها، رویکرد یکپارچه‌سازی محصولات سامانه مدیریت یکپارچه تهدیدات در سطح سازمانها مطرح می‌شود.

راه حل مدرن (ابزارهای امنیتی مجتمع)

مفهوم اولیه ابزارهای امنیتی مجتمع، مفهوم جدیدی نیست و به زبان ساده به معنای ترکیب چندین کارکرد امنیتی در یک راه حل یا ابزار واحد است. برخی از فروشندگان راه‌حل‌های امنیتی، ابزارهای امنیتی مجتمعی درگذشته ارائه کرده‌اند. با این‌وجود، این راه‌حل‌های جوان کمبودهای زیادی دارند. به‌خصوص اگر یکپارچه‌سازی کارکردها نامناسب بوده و به‌صورت ضعیفی اجرا شده باشد. این کمبودها می‌تواند شامل کارایی نامناسب، کاهش قابلیت اعتماد[1]، مقیاس‌پذیری محدود، افزایش پیچیدگی مدیریت و امنیت نامناسب باشد. به‌طورکلی رویه یکپارچه‌سازی کارکردهای امنیتی باید به‌گونه‌ای اجرا شود که فناوریهای مختلف استفاده‌شده بتوانند در کنار یکدیگر فعالیت کنند. نتیجه این یکپارچه‌سازی محصول Appliance خواهد شد که قابلیت توسعه سرویس‌های امنیتی جدید را خواهد داشت و برای مقابله با تهدیدات امروز و آینده از یک ساختار دفاع امنیتی لایه‌ای بهره‌مند است. هم‌چنین محصول نهایی در کنار توان دفاع امنیتی زیاد، باید بتواند ازلحاظ هزینه مقرون‌به‌صرفه باشد. در نمودار ۱ استفاده از راه‌حل یکپارچه‌سازی ساختارهای امنیتی در قالب یک محصول سامانه

1. Reliability

مدیریت یکپارچه تهدیدات در شبکه مورد نظر آورده شده است.



نمودار ۱. استفاده از راه‌حل یکپارچه‌سازی ساختارهای امنیتی در قالب یک محصول سامانه مدیریت یکپارچه تهدیدات

منبع: رضوانی (۱۳۸۶)

با در نظر گرفتن احتمال موفقیت UTM، تأثیرات ناشی از آن، هزینه واکنش‌های احتمالی و عوارض جانبی منفی واکنش‌ها، یک رویکرد کمی آگاهی‌دهنده از خطر را ارائه می‌کند که با ارائه احتمال جامع موفقیت تهدیدات، نمای کلی را در مورد تهدیدها ارائه می‌کند. واکنش‌ها بر اساس ارزیابیهای مالی، عملیاتی و تهدید به کاربران پیشنهاد می‌شود (گرادانیلو و همکاران[1]، ۲۰۱۸).

محصول سامانه مدیریت یکپارچه تهدیدات

بازار چشمگیر محصولات امنیتی سامانه مدیریت یکپارچه تهدیدات روند تولید محصولات تک‌کاربرد را به سمت ارائه چندین ویژگی امنیتی در یک سکو، و در محیط‌هایی منعطف‌تر می‌برد. به‌گفته چارلز کولوجی مدیر بخش تحقیقات محصولات امنیتی در سامانه مدیریت یکپارچه تهدیدات،

1. Granadillo et al.

IDC با ارائه برنامه‌های کاربردی امنیتی با کارایی زیاد و صرفه‌جویی در هزینه‌های عملیاتی و سرمایه، به‌سرعت در حال محبوب‌ترشدن است. طبق آمار IDC، بخش فروش سامانه مدیریت یکپارچه تهدیدات در گروه ابزارهای امنیت شبکه سریعترین رشد را در بازار داشته است (بیش از ۱۰۰ میلیون دلار سود در سال ۲۰۰۳ که با افزایش ۱۶۰ درصدی نسبت به سال ۲۰۰۲ همراه بود). طبق همین گزارش در سال ۲۰۰۸ از کل سود فروش ۳/۴۵ میلیارد دلاری دسته محصولات مدیریت امنیت شامل سامانه مدیریت یکپارچه تهدیدات، فایروال‌های سنتی و ابزارهای سامانه مدیریت یکپارچه تهدیدات، VPN به‌تنهایی ۵۸٪ سود فروش را خواهد داشت. همین پیش‌بینی نشان می‌دهد که سود فروش فایروال‌های سنتی رو به کاهش خواهد بود و این نشان از جایگزینی نیاز مشتریان در زمینه فایروال با محصولات سامانه مدیریت یکپارچه تهدیدات خواهد بود. بخشی از این پیش‌بینی در جدول ۱ آورده شده است.

جدول ۱. پیش‌بینی IDC در مورد رشد سود فروش سامانه مدیریت یکپارچه تهدیدات

بازه زمانی	۲۰۱۹	۲۰۲۰	۲۰۲۱	۲۰۲۲	۲۰۲۳	۲۰۲۴	۲۰۲۵
سامانه حفاظت UTM	۶۰۰۱	۶۵۰۰	۷۱۰۰	۷۴۳۵	۷۹۲۶	۸۴۲۰	۸۹۵۶
دیواره آتش/ حفاظت دستگاه	۱/۴۷۹	۱/۶۶۸	۱/۷۹۲	۱/۸۰۴	۱/۶۲۳	۱/۴۶۲	۱/۳۶۹

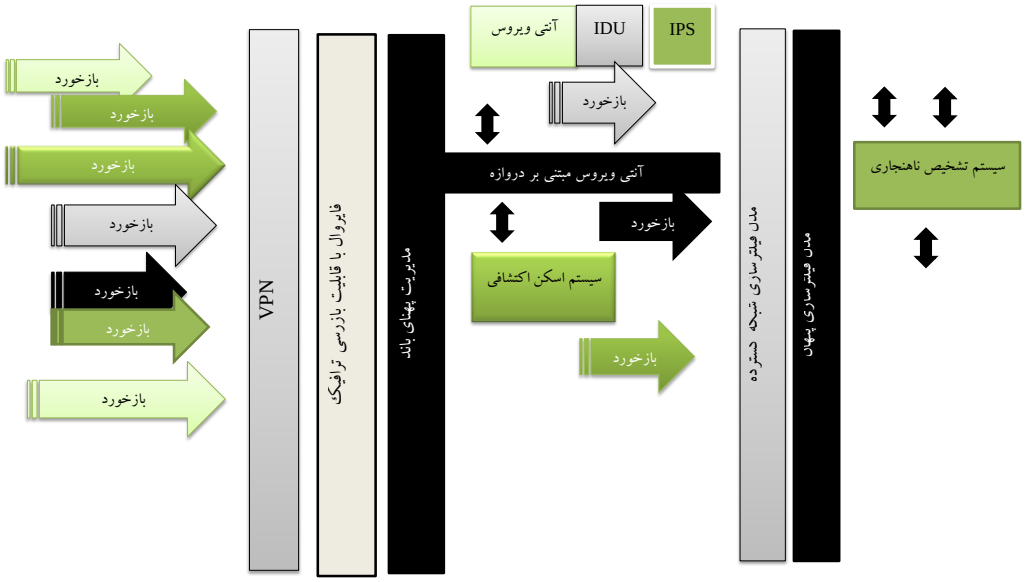
منبع: اینترنشنال دیتا کورپوریشن[1]

با توجه به رشد نیاز به محصولات سامانه مدیریت یکپارچه تهدیدات در بازار، فرایند تولید این محصول در بسیاری از شرکتهای تولیدکننده محصولات امنیتی شکل گرفته است. این فرایند در شرکتهای تولیدکننده محصولات Firewall/VPN با نگرش ارتقای محصول به سامانه مدیریت یکپارچه تهدیدات با سرعت بیشتری به نتیجه رسیده است، به‌طوری‌که بیشتر شرکتهای معتبر در زمینه تولید محصولات Firewall/VPN، امروزه محصول خود را برای تبدیل به سامانه مدیریت یکپارچه تهدیدات ارتقا داده و با این نام در بازار تجارت می‌کنند.

1. International Data Corporation (IDC)

معماری محصول

محصول سامانه مدیریت یکپارچه تهدیدات امنیت را در کل لایه‌های شبکه و به‌طور خاص در لایه محتوا ارائه می‌کند. برای این منظور باید چندین ساختار امنیتی را به‌صورت یکپارچه ارائه کند. این ساختارهای امنیتی شامل فایروال با قابلیت بازرسی حالت‌مند ترافیک، ارائه سرویس VPN با قراردادهای گوناگون، امکان تشخیص و جلوگیری از حمله (IPS)، آنتی‌ویروس مبتنی بر دروازه، فیلترینگ محتوای ترافیک (به‌طورمعمول برای محتوای Web و Mail ارائه می‌شود)، فیلترینگ اسپم روی ترافیک Mail و مدیریت پهنای باند است. نکته کلیدی در تولید محصولات سامانه مدیریت یکپارچه تهدیدات ارائه معماری مناسب برای چیدمان ساختارهای فوق است که بتواند بهترین کارایی را روی محصول ارائه کند. بدیهی است با افزایش میزان بازرسی ترافیک در راهبردهای امنیتی مختلف، امکان تأخیر و کاهش کارایی شبکه نمایان می‌شود. در این راستا استفاده از ایده‌هایی نظیر استفاده از شتاب‌دهنده‌های سخت‌افزاری می‌تواند برخی از مشکلات را مرتفع سازد. این ایده در بسیاری از شرکتهای بزرگ تولیدکننده محصولات امنیتی استفاده می‌شود. نمودار ۲ یک معماری نمونه از محصول سامانه مدیریت یکپارچه تهدیدات را نشان می‌دهد. چیدمان راهبردهای امنیتی و ترتیب بازرسی ترافیک در این محصول یکی از عوامل اصلی این معماری است. در این معماری اولین بازرسی امنیتی توسط ماژول حالت‌مند انجام می‌شود که به حذف بسیاری از تهدیدات منجر می‌شود. هم‌چنین این ایده می‌تواند به تولید مفهوم نشست برای بازرسی در ماژول‌های امنیتی دیگر منجر شود. از نکات دیگر این معماری قرار دادن بازرسی‌های محتوا در انتهای حرکت بسته است. این ایده به‌دلیل عدم نیاز به بازرسی محتوای ترافیک‌های مشکوک است. بدیهی است اگر ترافیکی توسط ماژول حالت‌مند متوقف شود، دیگر نیاز به بازرسی محتوایی توسط ماژول AntiSpam نیست.



نمودار ۲. جریان بازرسی ترافیک در یک محصول UTM

منبع: رضوانی (۱۳۸۶)

معماری ارائه شده در نمودار ۲ می‌تواند در یک محصول سامانه مدیریت یکپارچه تهدیدات مورد استفاده قرار گیرد ولی نکته کلیدی در اجرای این معماری ملاحظات پیاده‌سازی ارتباطات بین ماژول‌ها است. برای نمونه معماری ارائه‌شده در بالا هدف کاهش تعداد IPCها بین مؤلفه‌های محصول است. هم‌چنین نکته دیگری که در پیاده‌سازی این معماری باید در نظر گرفت، نوع الگوی مدیریتی است که محصول برای مدیر ارائه می‌کند (ینگ دار لین و همکاران[1]، ۲۰۰۶).

مزایای سامانه مدیریت یکپارچه تهدیدات

از مزایای سامانه مدیریت یکپارچه تهدیدات می‌توان به مدیریت یکپارچه (نظیر مدیریت چندین کاربر از یک محل و توسط یک ابزار، ایجاد و پیاده‌سازی آسان و سریع خط‌مشی‌های سراسر سازگار،

1. Ying-Dar Lin, Chih-Wei Jan, Po-Ching Lin, and Yuan-Cheng Lai,

تکیه بر گزاره‌ها و نظارت‌های برخط و تعاملی و استفاده از تنها یک واسط مستقیم برای نصب و مدیریت تمامی ویژگیهای امنیتی) اشاره کرد. سامانه مدیریت یکپارچه تهدیدات به‌عنوان یک محصول یکپارچه فرایند انتخاب محصولات امنیتی مورد نیاز، یکپارچه‌سازی آنها و پشتیبانی‌های آتی را ساده کرده است. محصولات سامانه مدیریت یکپارچه تهدیدات دارای مراحل نصب کم، ساده و عمدتاً به‌صورت plug and play هستند، ازآنجاکه کاربران عمدتاً تمایل به دست‌کاری تنظیمات دارند، در بسته‌هایی مانند ابزار سامانه مدیریت یکپارچه تهدیدات با کاهش تعامل اپراتور، خرابی‌های ایجادشده توسط آنها کاهش می‌یابد و در نتیجه امنیت افزایش می‌یابد، به‌دلیل اینکه تنها یک ابزار واسط امنیتی وجود دارد، در مواقع بروز مشکل برای عیب‌یابی، این وسیله حتی توسط یک فرد غیرمتخصص قابل خارج‌شدن از مدار است و هزینه لازم برای فراهم‌آوردن سطح امنیت مورد نیاز در سازمان توسط ابزارهای مجزای امنیتی بسیار بیشتر از هزینه راه‌حل سامانه مدیریت یکپارچه تهدیدات است. در مقایسه با راه‌حل‌های پیشین، UTM ورود به سامانه را آسان‌تر، ایمن‌تر و امن‌تر می‌کند (ناوان و بلرون[1]، ۲۰۱۹).

پیشینه پژوهش

در زمینه UTM تاکنون پژوهشی به‌صورت تجربی چه در ایران و چه خارج از ایران انجام نشده است. بیشتر پژوهشها در زمینه بحث فنی و مربوط به فناوری است و هیچ پژوهشی به شناسایی و رتبه عوامل مؤثر بر موفقیت نپرداخته است. این پژوهش علاوه بر تلفیق مدیریت و فناوری اطلاعات به بومی‌سازی محصولات نیز ارزش نهاده است. تنها پژوهش خارجی مرتبط با سامانه مدیریت یکپارچه تهدیدات پژوهش تام و همکاران[2] (۲۰۱۳) است. هم‌چنین در ایران هم پژوهشی به بررسی سامانه مدیریت یکپارچه تهدیدات نپرداخته است. ولی عمده پژوهشهایی که از دو روش تحلیل سلسله‌مراتبی فازی و تاپسیس فازی در پژوهشهای خود استفاده کرده‌اند به شرح ذیل است:

1. Navas & Beltrán
2. Tam et al.

جدول ۲. پیشینه پژوهش

پژوهشگر	سال	عنوان	یافته‌ها
تام و همکاران	(۲۰۱۳)	معرفی سامانه مدیریت یکپارچه تهدیدات	پژوهش به معرفی مفاهیم اساسی امنیت شبکه، مبانی مدیریت یکپارچه تهدیدات، حل مشکلات با مدیریت یکپارچه تهدیدات و چشم‌انداز بازار فعلی سامانه مدیریت یکپارچه تهدیدات پرداخته است
بخردی‌نسب و ژولانژاد	(۱۳۹۹)	تأثیر کیفیت مدیریت ریسک بر نوسانات ضمنی اعلان سود	نتایج نشان داده است که تغییرات در کیفیت مدیریت خطر، نوسانات ضمنی اعلان سود را کاهش می‌دهد.
آفرین محمدزاده و حسن‌زاده	(۱۳۹۷)	بررسی شناسایی و رتبه‌بندی عوامل مؤثر در پیاده‌سازی مدیریت زنجیره تأمین سبز با روش AHP فازی و TOPSIS فازی در صنعت برق	نتایج نشان داده است که شاخصهای توانایی تأمین مالی، افزایش ارتفاع برجها و دکلهای خطوط انتقال برق و هم‌چنین استفاده از انرژی تجدیدپذیر خورشیدی به‌ترتیب بیشترین وزن‌ها را به خود اختصاص داده‌اند.
بخردی‌نسب و ژولانژاد	(۱۳۹۶)	بررسی رفتار مدیر در برخورد با هزینه‌ها بر اساس رویکرد رتبه‌بندی شرکتها با مکانیزمهای حاکمیت شرکتی در تاپسیس فازی	نتایج نشان داده است چنانکه مدیریت، معیارهای حاکمیت شرکتی را همواره به‌صورت محسوس و نامحسوس بر رفتار خود ناظر قرار دهد، کمتر به اقدامات اختیاری و فرصت‌طلبانه دست می‌زنند.
باقری‌پیدنی و داودی	(۱۳۹۶)	بررسی شناسایی و رتبه‌بندی عوامل تأثیرگذار بر انتقال فناوری با استفاده از روش AHP فازی (بررسی موردی: شرکت فولاد مبارکه اصفهان)	نتایج نشان داده است که مهمترین معیار در زمینه انتقال فناوری شرکت فولاد مبارکه، سازمانهای بین‌المللی از زیرمجموعه شاخص اصلی ملاحظات قانونی و نظارتی است که براساس آن استفاده فنی و تأمین مالی از سازمانهای بین‌المللی و سازمانهای همکاری مشترک که قوانینی در جهت همکاریهای مشترک برای بهبود محیط‌زیست دارند، نقش مهمی در انتقال فناوری ایفا می‌کنند.
خیری	(۱۳۹۵)	بررسی شناسایی، تحلیل و رتبه‌بندی عوامل مؤثر کلیدی در پیاده‌سازی سامانه مدیریت امنیت اطلاعات در سازمانهای حاکمیتی (مطالعه موردی: سازمان بنادر و دریانوردی)	نتایج به‌دست آمده سازمان مرکزی را متقاعد کرد تا نسبت به برگزاری دوره‌های آموزشی مرتبط و بازآموزی موضوع سامانه امنیت اطلاعات و برنامه‌ریزی و تخصیص رسانه و نرم‌افزار اقدام کند.

ادامه جدول ۲. پیشینه پژوهش

پژوهشگر	سال	عنوان	یافته‌ها
فرهودی و همکاران	(۱۳۹۴)	بررسی شناسایی و اولویت‌بندی عوامل حیاتی موفقیت سامانه‌های اطلاعاتی در شرکت ملی پخش فرآورده‌های نفتی ایران با رویکرد برنامه‌ریزی راهبردی	یافته‌های این پژوهش نشان داده است که شش مضمون عوامل سازمانی، سیاسی، اجتماعی، اقتصادی، فرهنگی و فناورانه بزرگترین نقش در کسب موفقیت سامانه‌های اطلاعاتی شرکت را دارد و به‌ترتیب اولویت امنیت شبکه و سامانه‌ها، یکپارچه‌سازی پایگاه‌های داده، مدیر و نیروی انسانی توانمند، محوریت شایسته‌سالاری، هم‌راستایی راهبردهای فناوری اطلاعات با کسب و کار، رابطه بین رهبر و کارکنان و پذیرش سامانه‌ها توسط مدیریت ارشد از مؤثرترین عوامل در نتیجه این پژوهش هستند.

منبع: یافته‌های پژوهشگر

با بررسی پیشینه پژوهش می‌توان دریافت که تاکنون هیچ پژوهشگری چه داخلی و چه خارجی به بررسی و تحلیل سامانه مدیریت یکپارچه تهدیدات نپرداخته است. پس خلاء و شکاف موجود، عدم شناسایی نقاط قوت و ضعف سامانه مدیریت یکپارچه تهدیدات است که به‌عنوان محرک انجام این پژوهش بوده است. این پژوهش با انتخاب نمونه‌آماری و تعمیم آن به کل جامعه‌آماری، قصد دارد تا عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات را شناسایی و الویت‌بندی، و نسبت به رفع این شکاف اقدام کند.

۳. روش‌شناسی پژوهش

در این بخش به بررسی روش پژوهش، سؤالها، جامعه و نمونه آماری، و روش اجرا پرداخته شده است.

روش پژوهش

این پژوهش از نظر هدف، کاربردی، از دید روش، از انواع پژوهشهای پیمایشی، ازلحاظ چگونگی گردآوری داده‌ها، توصیفی پیمایشی و به لحاظ زمانی، تک‌مقطعی و به‌طور مشخص بر ترکیبی از روشهای تصمیم‌گیری چند معیاره مبتنی است.

سؤال‌های پژوهش

چه عواملی بر موفقیت سامانه مدیریت یکپارچه تهدیدات تأثیرگذارند؟

عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات از چه رتبه‌ای برخوردارند؟

جامعه آماری و حجم نمونه

جامعه آماری این پژوهش را کارکنان شرکت امن‌پردازان کویر تشکیل می‌دهد. شرکت امن‌پردازان کویر شش شرکت تولیدکننده سامانه مدیریت یکپارچه تهدیدات بومی با تأییدیه سازمان فناوری اطلاعات دارد. هر شرکت ۱۰ نیروی متخصص از مدیران، کارشناسان ارشد و کارشناسان متخصص دارد. سؤالها به صورت برخط بر روی سامانه شرکت قرار گرفت و از بین ۶۰ نفر مدیران، کارشناسان ارشد و کارشناسان متخصص شرکت امن‌پردازان کویر، ۵۰ نفر پاسخگوی سؤال‌های پژوهش بودند. بازه زمانی پژوهش بهار و تابستان ۱۳۹۷ بود.

روش اجرا

به‌منظور تجزیه و تحلیل داده‌ها از ترکیب روشهای تصمیم‌گیری در وضعیت نبود اطمینان استفاده شده است. در این روش با استفاده از نظر کارشناسان و خبرگان معیارهایی به‌منظور شناسایی عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات شناسایی شد؛ سپس با توجه به وزندهی به معیارهای شناسایی‌شده، عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات رتبه‌بندی شد. با مطالعه کتابها و مقالات داخلی و خارجی، تعدادی شاخص برای دستیابی به عوامل موفقیت سامانه مدیریت یکپارچه تهدیدات به‌دست می‌آید که در مرحله بعدی به کمک پرسشنامه‌هایی که در اختیار کارشناسان قرار می‌گیرد و با در نظر گرفتن محدودیتها، چهار معیار نهایی، قطعی شد. سپس این معیارها با استفاده از پرسشنامه برخط، مقایسات زوجی که در اختیار خبرگان قرار گرفته است وزن‌دهی و وزن هر شاخص مشخص می‌شود. عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات شناسایی‌شده به‌شرح جدول ۳ است.

جدول ۳. عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات شناسایی‌شده

معیارها	عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات
عوامل فردی	استقامت و پشتکار کارکنان
عوامل فردی	اعتمادبه‌نفس کارکنان
عوامل فردی	ایده و تفکرات نوین مدیران
عوامل فردی	تجربه مدیران
عوامل فردی	تحصیلات دانشگاهی کارکنان
عوامل فردی	خلاقیت و نوآوری مدیران
عوامل فردی	رقابت‌پذیری مدیران در پذیرش رقیبان
عوامل فردی	خطرپذیری کارکنان
عوامل فردی	شهامت و شجاعت کارکنان
عوامل فردی	صداقت و درستی اعضا
عوامل فردی	فروتنی اعضا
عوامل فردی	قدرت انعطاف‌پذیری
عوامل فردی	مسئولیت‌پذیری
عوامل فردی	مهارت
عوامل فردی	هوش و استعدادها
عوامل عملکردی	انجام وظایف مدیران به نحو احسن
عوامل عملکردی	انجام وظایف هریک از اعضا در سازمان به نحو احسن
عوامل عملکردی	آینده‌نگری
عوامل عملکردی	تقسیم‌کار
عوامل عملکردی	مدیریت زمان
عوامل سازمانی	اختیار عمل اعضا
عوامل سازمانی	آموزشهای ضمن خدمت به اعضا در سازمان
عوامل سازمانی	اهداف سازمانی از پیش تعیین‌شده
عوامل سازمانی	فرهنگ و جوسازمانی
عوامل سازمانی	برنامه‌های انگیزشی در سازمان
عوامل سازمانی	ساختار سازمانی
عوامل سازمانی	منابع سازمانی
عوامل محیطی	استفاده از فناوری روز
عوامل محیطی	رفتار و عکس‌العمل رقبا
عوامل محیطی	عوامل اقتصادی
عوامل محیطی	عوامل فرهنگی و اجتماعی
عوامل محیطی	عوامل قانونی و سیاسی

به‌طور کلی هدف این است که پس از تعیین معیارها و شاخصهای مورد نظر با توجه به مطالعه کتابها و مقالات داخلی و خارجی مرتبط و هم‌چنین نظر خبرگان و کارشناسان، با کمک فرایند تحلیل سلسله مراتبی فازی به هر کدام از معیارها وزنی اختصاص داده شود. در مرحله بعد با استفاده از روش تاپسیس فازی، گزینه‌های مورد نظر با توجه به وزن تعیین‌شده، رتبه‌بندی می‌شود.

ابزار سنجش

در این پژوهش از چهار پرسشنامه به‌صورت مرحله به مرحله استفاده شده است. کارشناسانی که به پرسشنامه‌ها پاسخ دادند از مدیران، کارشناسان ارشد و کارشناسان متخصص هستند. پرسش‌های چهار معیار اصلی به شرح جدول ۴ است.

جدول ٤. پرسشنامه

عوامل فردی مؤثر بر موفقیت سامانه مدیریت
۱. آیا مهارتها در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۲. آیا مسئولیت‌پذیریها در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۳. آیا اعتماد به نفس کارکنان در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۴. آیا شهامت و شجاعت کارکنان در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۵. آیا صداقت و درستی اعضا در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۶. آیا فروتنی اعضا در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۷. آیا استقامت و پشتکار کارکنان در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۸. آیا قدرت انعطاف‌پذیری در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۹. آیا تجربه مدیران در پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۱۰. آیا هوش و استعدادها در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۱۱. آیا تحصیلات دانشگاهی کارکنان در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۱۲. آیا خطرپذیری کارکنان در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۱۳. آیا رقابت‌پذیری مدیران در پذیرش رقیبان در پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۱۴. آیا خلاقیت و نوآوری مدیران در پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۱۵. آیا تفکرات نوین مدیران در راستای پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟

ادامه جدول ٤. پرسشنامه

عوامل عملکردی مؤثر بر موفقیت سامانه مدیریت
۱. آیا انجام وظایف مدیران به نحو احسن در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۲. آیا انجام وظایف هریک از اعضا در سازمان به نحو احسن بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۳. آیا آینده نگری در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۴. آیا مدیریت زمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۵ آیا تقسیم کار بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
عوامل سازمانی مؤثر بر موفقیت سامانه مدیریت
۱. آیا اختیار عمل اعضا در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۲. آیا اهداف سازمانی از پیش‌تعیین‌شده بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۳. آیا فرهنگ و جو سازمانی بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۴. آیا ساختار سازمانی بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۵. آیا منابع سازمانی بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۶. آیا برنامه‌های انگیزشی در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۷. آیا آموزشهای ضمن خدمت به اعضا در سازمان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
عوامل محیطی مؤثر بر موفقیت سامانه مدیریت
۱. آیا عوامل اقتصادی بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۲. آیا عوامل فرهنگی و اجتماعی بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۳. آیا عوامل قانونی و سیاسی بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۴. آیا استفاده از فناوری روز بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟
۵. آیا رفتار و واکنش رقیبان بر پیاده‌سازی سامانه مدیریت یکپارچه تأثیر دارد؟

به‌منظور تعیین اهمیت هر یک از معیارها از مقیاس لیکرت استفاده شد. در این بخش از پژوهش برای آزمایش اولیه تعداد ۵۵ پرسشنامه طی دو مرحله بین خبرگان و متخصصان توزیع شد. در پرسشنامه اول از کارشناسان خواسته شده نظرشان را در مورد اهمیت معیارهای استخراج‌شده از کتابها و مقالات با پاسخ بلی یا خیر مشخص کنند، و در نهایت اگر معیار دیگری به‌نظرشان می‌رسد در انتها اضافه کنند. روایی پرسشنامه‌ها توسط خبرگان مورد تأیید قرار گرفته و پایایی آن نیز با محاسبه نرخ ناسازگاری بررسی شده است. میزان بار عاملی مقیاس لیکرت به‌صورت خیلی زیاد (میزان عامل

اندازه‌گیری عدد ۵)، زیاد (میزان عامل اندازه‌گیری عدد ۴)، متوسط (میزان عامل اندازه‌گیری عدد ۳)، کم (میزان عامل اندازه‌گیری عدد ۲) و خیلی کم (میزان عامل اندازه‌گیری عدد ۱) است. بدین‌منظور نمونه‌های اولیه شامل نمونه‌های ۲۵نفره و ۳۰نفره دوبار پرسشنامه پیش‌آزمون را تکمیل کردند و سپس با استفاده از داده‌های به‌دست‌آمده از این پرسشنامه‌ها و به کمک نرم‌افزار آماری SPSS 21 میزان ضریب اعتماد با روش آلفای کرونباخ به شرح جدول ۵ محاسبه شد.

جدول ۵. میزان آلفای کرونباخ

معیارها	تعداد سؤالها	آلفای کرونباخ نمونه ۲۵ نفره	آلفای کرونباخ نمونه ۳۰ نفره
عوامل فردی	۱۵	۰/۹۱۶	۰/۹۱۴
عوامل عملکردی	۵	۰/۹۳۶	۰/۹۲۷
عوامل سازمانی	۷	۰/۷۳۷	۰/۷۲۱
عوامل محیطی	۵	۰/۸۴۷	۰/۸۵۸

ازآنجاکه مقدار به‌دست‌آمده آلفای کرونباخ برای همه متغیرهای تحقیق از ۰/۷ بیشتر است می‌توان گفت پرسشنامه از پایایی قابل قبولی برخوردار است.

الگوی تحلیل سلسله مراتبی فازی

هایلرهون و پدر (۱۹۸۳) روشی برای فرایند تحلیل سلسله مراتبی فازی پیشنهاد کردند که بر اساس حداقل مجذورات لگاریتمی بنا شده است؛ اما تعداد محاسبات و پیچیدگی مراحل این روش باعث شد که چندان مورد استفاده قرار نگیرد. چانگ (۱۹۹۶) روش تحلیل توسعه‌ای را ارائه کرد. اعداد به‌کار رفته در این روش، اعدا فازی مثلثی هستند (مؤمنی، ۱۳۸۹). در این روش برای هر یک از سطرهای ماتریس مقایسه‌های زوجی، یک عدد فازی مثلثی محاسبه می‌شود. در جدول ۶ مقایسه کلامی و اعداد فازی مثلثی مربوط به آنها که برای انجام مقایسه‌های زوجی به‌کار می‌رود، ارائه شده است. تصمیم‌گیرندگان از مجموعه کلامی زیر برای وزن‌دهی استفاده کردند: حاصل‌ضرب دو عدد فازی مثلثی یا معکوس یک عدد فازی مثلثی، دیگر یک عدد فازی مثلثی نیست و این روابط فقط تقریبی از حاصل‌ضرب واقعی دو عدد فازی مثلثی و معکوس یک عدد فازی مثلثی را بیان می‌کند.

جدول ٦. متغیرهای کلامی و اعداد فازی مثلثی

مقیاس فازی مثلثی طرف مقابل	مقیاس فازی مثلثی	مقیاس کلامی اهمیت نسبی	عدد فازی
۰/۳۳ ۱ ۱	۱ ۱ ۳	اهمیت یکسان	۱
۱ ۰/۳۳ ۰/۲	۱ ۳ ۵	نسبتاً با اهمیت	۳
۰/۱۴ ۰/۲ ۰/۳۳	۳ ۵ ۷	با اهمیت	۵
۰/۱۱ ۰/۱۴ ۰/۲	۵ ۷ ۹	اهمیت زیاد	۷
۰/۱۱ ۰/۱۱ ۰/۱۴	۷ ۹ ۹	کاملاً با اهمیت	۹

جدول ۷ مربوط به مقیاسهای کلامی و اعداد فازی مرتبط با آنها است.

جدول ۷. مقیاس کلامی مورد استفاده در پژوهش برای سنجش درجه اهمیت نسبی

متغیرهای زبانی	اعداد فازی
خیلی ضعیف	(۱ ۱ ۳)
ضعیف	(۱ ۳ ۵)
متوسط	(۳ ۵ ۷)
خوب	(۵ ۷ ۹)
خیلی خوب	(۷ ۹ ۹)

تاپسیس فازی

روش تاپسیس به‌عنوان یکی از روشهای بسیار کاربردی و عملی در روشهای تصمیم‌گیری با معیارهای چندگانه کلاسیک توسط هوانگ و یون (۱۹۸۱) به‌منظور تجزیه و تحلیل راه‌حلهای جایگزین در میان هر معیار و درنهایت تعیین کارامدترین جایگزین‌ها ارائه شد. الگوریتم تاپسیس براساس کوتاه‌ترین فاصله از راه حل ایده‌آل مثبت و دورترین فاصله از راه‌حل ایده‌آل منفی سرچشمه گرفته است (پاتیل و کانت، ۲۰۱۴). اغلب برای تصمیم‌گیرندگان تخصیص یک امتیاز ارزیابی دقیق به یک جایگزین دشوار است، مزیت استفاده از روش فازی غلبه بر ابهام در قضاوتهای انسانی و به‌دست‌آوردن اهمیت نسبی صفات است (یانگ و هونگ، ۲۰۰۷). مراحل اجرای این روش شامل ۹ گام اساسی است. گام اول به تخصیص امتیاز با مقیاس زبانی به گزینه‌ها باتوجه به هر معیار می‌پردازد. گام دوم امتیاز فازی کل برای جایگزین‌ها محاسبه می‌شود. در گام سوم ماتریس تصمیم فازی محاسبه

می‌شود. در گام چهارم داده‌های خام با استفاده از یک تبدیل مقیاس خطی به‌منظور تبدیل مقیاسهای متنوع برای معیارها به مقیاسهای قابل مقایسه نرمالیز (به‌هنجار) تبدیل می‌شود. محاسبه ماتریس نرمالیز وزین در گام پنجم انجام می‌شود. محاسبه راه حل ایده‌آل مثبت و راه حل ایده‌آل منفی برای جایگزین‌ها در گام ششم انجام می‌شود. فاصله هر جایگزین از راه حل ایده‌آل مثبت و راه حل ایده‌آل منفی در گام هفتم محاسبه می‌شود. ضریب نزدیکی هر جایگزین در گام هشتم محاسبه می‌شود. ضریب نزدیکی فاصله نسبت به راه حل ایده‌آل مثبت فازی و راه حل ایده‌آل منفی را به صورت هم‌زمان نشان می‌دهد. درنهایت در گام نهم رتبه‌بندی جایگزین‌ها انجام می‌شود. در این مرحله جایگزین‌های مختلف مطابق با مقدار ضر یب نزدیکی رتبه‌بندی می‌شود.

٤. یافته‌های پژوهش

یافته‌های پژوهش شامل دو بخش شناسایی عوامل مؤثر بر موفقیت با استفاده از تحلیل سلسله مراتبی فازی و رتبه‌بندی عوامل مؤثر بر موفقیت با استفاده از روش تاپسیس فازی است که در ادامه ارائه شده است.

شناسایی عوامل مؤثر بر موفقیت با استفاده از تحلیل سلسله مراتبی فازی

با استفاده از آزمون علامت، رتبه چهار گروه عوامل مؤثر بر موفقیت مشخص شد که نتایج آن در جدول ۸ ارائه شده است.

جدول ۸. عوامل و میانگین رتبه‌ها

عوامل	تعداد	میانگین رتبه
عوامل فردی	۴۱	۹۵/۲۴
عوامل عملکردی	۴۳	۹۳/۶۳
عوامل سازمانی	۴۳	۷۸/۷۳
عوامل محیطی	۴۲	۷۲/۵۸

بین چهار گروه مورد بررسی تفاوت معناداری وجود ندارد و به‌طور متوسط همه عوامل (عوامل فردی، عوامل عملکردی، عوامل سازمانی، عوامل محیطی) رتبه برابر دارد. نتایج آزمون علامت در جدول ۹ ارائه شده است.

جدول ۹. آزمون علامت

آماره	مقدار
آماره کای دو	۶/۵۶۷
درجه آزادی	۳
سطح معناداری	۰/۰۸۷

نتایج فرایند تحلیل سلسله مراتبی فازی برای چهار گروه عوامل مؤثر بر موفقیت نشان می‌دهد که نتایج رتبه‌بندی متفاوت است و میزان اهمیت آنها به این‌صورت است که عوامل فردی و عوامل عملکردی با وزن ۰/۲۵۵ بیشترین اهمیت را دارد و عوامل محیطی با وزن ۰/۲۴۳ کمترین رتبه یا اندازه را دارد. نتایج حاصل از یافته‌ها در جدول ۱۰ ارائه شده است.

جدول ۱۰. نتایج حاصل از روش تحلیل سلسله‌مراتبی فازی برای رتبه‌بندی عوامل

عامل	اندازه	رتبه
عوامل فردی	۰/۲۵۵	اول
عوامل عملکردی	۰/۲۵۵	اول
عوامل سازمانی	۰/۲۴۶	دوم
عوامل محیطی	۰/۲۴۳	سوم

تاکنون نتایج نشان می‌دهد که با استفاده از روش تحلیل سلسله مراتبی فازی می‌توان عوامل را رتبه‌بندی کرد و نتایج بهتری مشاهده کرد. در این پژوهش با استفاده از روش آزمون علامت به رتبه‌بندی عوامل قادر نبودیم؛ اما با استفاده از روش تحلیل سلسله مراتبی فازی می‌توان نتایج بهتری برای مقایسه عوامل نسبت به همدیگر به‌دست آورد. پس می‌توان بیان کرد که روش تحلیل سلسله مراتبی فازی برای پیاده‌سازی سامانه مدیریت یکپارچه تهدیدات مؤثر است.

رتبه‌بندی عوامل مؤثر بر موفقیت با استفاده از روش تاپسیس فازی

در این بخش ابتدا با استفاده از آزمون فریدمن مؤلفه‌های هر عامل را مقایسه و رتبه‌بندی کرده و سپس با کمک روش تاپسیس فازی باز دوباره مؤلفه‌های هر عامل را رتبه‌بندی کرده و نتایج باهم

مقایسه می‌شود. در ادامه هرکدام از عوامل چهارگانه رتبه‌بندی بر اساس آزمون فریدمن دسته‌بندی شده است. بر اساس آزمون فریدمن برای عامل فردی عامل مهارت با میانگین رتبه ۱۱/۱۳ اولین است؛ دیگر اطلاعات تکمیلی در جدول ۱۱ ارائه شده است.

جدول ۱۱. رتبه‌بندی عوامل فردی بر اساس آزمون فریدمن

گویه	میانگین گویه	رتبه
مهارت	۱۱/۱۳	اول
مسئولیت‌پذیری	۱۱/۱۲	دوم
اعتمادبه‌نفس کارکنان	۹/۰۵	ششم
شهامت و شجاعت کارکنان	۹/۰۷	پنجم
صداقت و درستی اعضا	۱۰/۶۰	سوم
فروتنی اعضا	۴/۴۰	پانزدهم
استقامت و پشتکار کارکنان	۶/۹۱	نهم
قدرت انعطاف‌پذیری	۸/۰۹	هفتم
تجربه مدیران	۱۰/۴۰	چهارم
هوش و استعدادها	۶/۶۲	دوازدهم
تحصیلات دانشگاهی کارکنان	۶/۱۵	سیزدهم
خطرپذیری کارکنان	۵/۴۶	چهاردهم
رقابت‌پذیری مدیران در پذیرش رقیبان	۶/۸۳	یازدهم
خلاقیت و نوآوری مدیران	۶/۸۹	دهم
ایده و تفکرات نوین مدیران	۷/۲۷	هشتم

با توجه به آماره‌های آزمون فریدمن که در جدول ۱۱ ارائه شده است، این آزمون برای عوامل فردی معنادار است و رتبه‌بندی عوامل آن به‌صورت جدول ۱۲ است.

جدول ۱۲. نتایج آماری عوامل فردی آزمون فریدمن

آماره	اندازه
آماره کای دو	۱۶۲/۴۳
درجه آزادی	۱۴
سطح معناداری	۰/۰۰۰

در ادامه بر اساس آزمون فریدمن برای عامل عملکردی انجام وظایف مدیران به نحو احسن با میانگین رتبه ۳/۴۹ اولین است؛ دیگر اطلاعات تکمیلی در جدول ۱۳ ارائه شده است.

جدول ۱۳. رتبه‌بندی عوامل عملکردی بر اساس آزمون فریدمن

گویه	میانگین گویه	رتبه
انجام وظایف مدیران به نحو احسن	۳/۴۹	اول
انجام وظایف هریک از اعضا در سازمان به نحو احسن	۳/۰۹	دوم
آینده‌نگری	۲/۷۰	پنجم
مدیریت زمان	۲/۹۷	سوم
تقسیم‌کار	۲/۷۶	چهارم

با توجه به آماره‌های آزمون فریدمن که در جدول ۱۴ ارائه شده است، این آزمون برای عوامل عملکردی معنادار است و رتبه‌بندی عوامل آن به‌صورت جدول ۱۴ است.

جدول ١٤. نتایج آماری آزمون فریدمن برای عوامل عملکردی

آماره	اندازه
آماره کای دو	۹/۴۵
درجه آزادی	۴
سطح معناداری	۰/۰۵۱

هم‌چنین بر اساس آزمون فریدمن برای عامل سازمانی ساختار سازمانی با میانگین رتبه ۴/۵۶ اولین است؛ دیگر اطلاعات تکمیلی در جدول ۱۵ ارائه شده است.

جدول ۱۵. رتبه‌بندی عوامل سازمانی بر اساس آزمون فریدمن

گویه	میانگین گویه	رتبه
اختیار عمل اعضا	۳/۲۰	هفتم
اهداف سازمانی از پیش تعیین‌شده	۴/۲۳	دوم
فرهنگ و جو سازمانی	۴/۲۰	سوم
ساختار سازمانی	۴/۵۶	اول
منابع سازمانی	۴/۰۳	پنجم
برنامه‌های انگیزشی در سازمان	۳/۶۵	ششم
آموزش‌های ضمن خدمت به اعضا در سازمان	۴/۱۳	چهارم

با توجه به آماره‌های آزمون فریدمن که در جدول ۱۶ ارائه شده است، این آزمون برای عوامل سازمانی معنادار است و رتبه‌بندی عوامل آن به‌صورت جدول ۱۷ است.

جدول ۱٦. نتایج آماری برای عوامل سازمانی آزمون فریدمن

آماره	اندازه
آماره کای دو	۱۶/۵۱
درجه آزادی	۶
سطح معناداری	۰/۰۱۱

در انتها بر اساس آزمون فریدمن برای عامل محیطی استفاده از فناوری روز با میانگین رتبه ۳/۴۳ اولین است ؛ دیگر اطلاعات تکمیلی در جدول ۱۷ نمایش داده شده است.

جدول ۱۷. رتبه‌بندی عوامل محیطی بر اساس آزمون فریدمن

گویه	میانگین گویه	رتبه
عوامل اقتصادی	۲/۹۹	سوم
عوامل فرهنگی و اجتماعی	۲/۴۹	پنجم
عوامل قانونی و سیاسی	۲/۷۷	چهارم
استفاده از فناوری روز	۳/۴۳	اول
رفتار و عکس‌العمل رقبا	۳/۳۳	دوم

با توجه به آماره‌های آزمون فریدمن که در جدول ۱۸ ارائه شده است این آزمون برای عوامل محیطی معنادار است و رتبه‌بندی عوامل آن به‌صورت جدول ۱۹ است.

جدول ۱۸. نتایج آماری عوامل محیطی آزمون فریدمن

آماره	اندازه
آماره کای دو	۱۴/۴۳
درجه آزادی	۴
سطح معناداری	۰/۰۰۶

در انتهای این بخش رتبه‌بندی مؤلفه‌های هر یک از عوامل چهارگانه مؤثر بر موفقیت با استفاده از روش تاپسیس فازی انجام شده است. نتایج به‌کارگیری روش تاپسیس فازی نشان می‌دهد از بین مؤلفه‌های مربوط به عوامل فردی مؤثر بر موفقیت سامانه مدیریت، مؤلفه مهارت، مؤثرترین مؤلفه در عوامل فردی است. درجه تأثیرگذاری مؤلفه‌های دیگر در جدول ۲۰ آمده است.

جدول ۱۹. رتبه‌بندی مؤلفه‌های مربوط به عوامل فردی مؤثر بر موفقیت سامانه مدیریت

عوامل فردی مؤثر بر موفقیت سامانه مدیریت	فاصله با ایده‌آل مثبت	فاصله با ایده‌آل منفی	Ci	رتبه
مهارت	۱۹۸/۵۷	۲۳۹/۰۱	۰/۵۴۶۲	اول
مسئولیت‌پذیری	۲۰۳/۹۳	۲۳۲/۲۳	۰/۵۳۲۴	دوم
اعتمادبه‌نفس کارکنان	۲۲۶/۱۳	۱۹۸/۵۸	۰/۴۶۷۵	دهم
شهامت و شجاعت کارکنان	۲۳۹/۱۱	۱۷۱/۲۴	۰/۴۱۷۳	چهاردهم
صداقت و درستی اعضا	۲۰۹/۲۸	۲۲۶/۸۱	۰/۵۲۰۱	چهارم
فروتنی اعضا	۲۷۳/۸۹	۱۳۲/۱۶	۰/۳۲۵۴	پانزدهم
استقامت و پشتکار کارکنان	۲۲۴/۱۷	۲۱۴/۶۹	۰/۴۸۹۱	هفتم
قدرت انعطاف‌پذیری	۲۱۸/۹۳	۲۲۰/۹۲	۰/۵۰۲۲	پنجم
تجربه مدیران	۲۰/۴۲	۲۳۳/۱۸	۰/۵۳۰۴	سوم
هوش و استعدادها	۲۲۸/۲۴	۲۱۰/۸۱	۰/۴۸۰۱	هشتم
تحصیلات دانشگاهی کارکنان	۲۳۷/۸۶	۱۹۸/۰۳	۰/۴۵۴	یازدهم
خطرپذیری کارکنان	۲۴۸/۱	۱۸۵/۵۹	۰/۴۲۷۹	سیزدهم
رقابت‌پذیری مدیران در پذیرش رقیبان	۲۲۸/۹۴	۲۰۹/۴۶	۰/۴۷۷۷	نهم
خلاقیت و نوآوری مدیران	۲۳۴/۳۳	۱۹۳/۵	۰/۴۵۲۲	دوازدهم
ایده و تفکرات نوین مدیران	۲۲۹/۴۵	۲۲۶/۷۶	۰/۴۹۷	ششم

همان‌طور که جدول ۲۰ نشان می‌دهد، از بین مؤلفه‌های مربوط به عوامل عملکردی مؤثر بر موفقیت سامانه مدیریت، مؤلفه‌های انجام وظایف مدیران به‌نحو احسن، انجام وظایف هر یک از اعضا در سازمان به‌نحو احسن و آینده‌نگری بااهمیت‌ترین شاخص‌ها برای بهبود عوامل عملکردی مؤثر بر موفقیت سامانه مدیریت است.

جدول ۲۰. رتبه‌بندی مؤلفه‌های مربوط به عوامل عملکردی مؤثر بر موفقیت سامانه مدیریت

عوامل عملکردی مؤثر بر موفقیت سامانه مدیریت	فاصله با ایده‌آل مثبت	فاصله با ایده‌آل منفی	Ci	رتبه
انجام وظایف مدیران به نحو احسن	۱۶۰/۱۶	۱۶۳/۸	۰/۵۰۵۶	اول
انجام وظایف هریک از اعضا در سازمان به نحو احسن	۱۶۲/۴۸	۱۶۴/۵۵	۰/۵۰۳۱	دوم
آینده‌نگری	۱۷۰/۶۶	۱۵۴/۱۶	۰/۴۷۴۵	سوم
مدیریت زمان	۱۷۱/۷۵	۱۵۱/۴۱	۰/۴۶۸۵	چهارم
تقسیم‌کار	۱۷۲/۵۷	۱۵۲/۱۳	۰/۴۶۸۵	چهارم

هم‌چنین نتایج حاصل از اولویت‌بندی مؤلفه‌های مربوط به عوامل سازمانی مؤثر بر موفقیت سامانه مدیریت در شرکت امن‌پرداز کویر با استفاده از روش تاپسیس فازی نشان می‌دهد، ساختار سازمانی نسبت به دیگر مؤلفه‌های مربوط به عوامل سازمانی، بیشترین تأثیر را دارد.

جدول ۲۱. رتبه‌بندی مؤلفه‌های مربوط به عوامل سازمانی مؤثر بر موفقیت سامانه مدیریت

عوامل سازمانی مؤثر بر موفقیت سامانه مدیریت	فاصله با ایده‌آل مثبت	فاصله با ایده‌آل منفی	Ci	رتبه
اختیار عمل اعضا	۲۴۴/۸۶	۱۷۴/۴۲	۰/۴۱۶	هفتم
اهداف سازمانی از پیش تعیین‌شده	۲۱۹/۷۸	۲۰۴/۶۱	۰/۴۸۲۱	سوم
فرهنگ و جو سازمانی	۲۱۹/۷	۱۹۴/۷۸	۰/۴۶۹۳	چهارم
ساختار سازمانی	۲۱۳/۳۲	۲۱۰/۶۹	۰/۴۹۶۹	اول
منابع سازمانی	۲۱۹/۱۸	۲۰۵/۱۴	۰/۴۸۳۴	دوم
برنامه‌های انگیزشی در سازمان	۲۳۷/۱۷	۱۷۳/۱۹	۰/۴۲۲۰	ششم
آموزشهای ضمن خدمت به اعضا در سازمان	۲۲۶/۴۳	۱۹۵/۰۹	۰/۴۶۲۸	پنجم

هم‌چنین نتایج حاصل از به‌کارگیری روش تاپسیس فازی در جدول ۲۱ نشان می‌دهد از بین مؤلفه‌های مربوط به عوامل محیطی مؤثر بر موفقیت سامانه مدیریت، به‌ترتیب مؤلفه‌های عوامل اقتصادی، عوامل فرهنگی و اجتماعی و عوامل قانونی و سیاسی تأثیرگذارترین مؤلفه‌ها بر ارتقای شناسایی و رتبه‌بندی عوامل مؤثر بر موفقیت هستند.

جدول ۲۲. رتبه‌بندی مؤلفه‌های مربوط به عوامل محیطی مؤثر بر موفقیت سامانه مدیریت

عوامل محیطی مؤثر بر موفقیت سامانه مدیریت	فاصله با ایده‌آل مثبت	فاصله با ایده‌آل منفی	Ci	رتبه
عوامل اقتصادی	۱۷۲/۰۷	۱۶۰/۷۲	۰/۵۲۳۳	اول
عوامل فرهنگی و اجتماعی	۱۹۵/۶۸	۱۳۱/۲۶	۰/۴۸۳۶	دوم
عوامل قانونی و سیاسی	۱۸۱/۸۸	۱۴۸/۶۳	۰/۴۸۲۹	سوم
استفاده از فناوری روز	۱۵۹/۷۱	۱۵۷/۳۷	۰/۴۴۹۷	چهارم
رفتار و عکس‌العمل رقیبان	۱۷۱/۸۱	۱۶۰/۹۵	۰/۴۰۱۴	پنجم

بر اساس نتایج بین رتبه‌بندی براساس روش فریدمن و تاپسیس فازی تفاوت معناداری وجود دارد و رتبه‌بندی بر اساس این دو روش با همدیگر تفاوت دارند. پس رتبه‌بندی عوامل مؤثر بر موفقیت برای پیاده‌سازی سامانه مدیریت یکپارچه تهدیدات در شرکت امن‌پردازان کویر مؤثر است و تفاوت بین روشهای تحلیل سلسله مراتبی فازی و رتبه‌بندی عوامل مؤثر بر موفقیت برای پیاده‌سازی سامانه مدیریت یکپارچه تهدیدات در شرکت امن‌پردازان کویر معنادار است.

۵. بحث و نتیجه‌گیری

تهدیدات اینترنتی هر روز پیچیده‌تر و فزاینده‌تر از قبل به شبکه‌های رایانه‌ای هجوم می‌آورند و همین مسئله نیاز به راه‌کارهای جدیدتر و پیشرفته‌تر برای افزایش توان دفاعی مراکز سازمانی را به‌شدت افزایش داده است. از طرفی روشهای سنتی و قدیمی حفاظت از اطلاعات رایانه‌ای، در برابر روشهای جدید تخریب و نفوذ و سرقت اطلاعات بی‌اثر و بی‌فایده است و باید همواره داده‌ها و اطلاعات را در سطحی بالا از امنیت قرار داد تا بتوان این آسیب‌پذیریها را از بین برد یا تا حد بسیار

زیادی کاهش داد. در این راستا استفاده از سخت‌افزارهای یکپارچه‌سازی می‌تواند راه‌کار مناسبی به‌منظور دستیابی به این اهداف باشد. ولی در کنار استفاده از سامانه مدیریت یکپارچه تهدیدات، مدیریت باید بداند که چه عواملی بر موفقیت سامانه مدیریت یکپارچه تهدیدات تأثیرگذار است. بر این اساس این پژوهش به بررسی شناسایی و رتبه‌بندی عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات پرداخت. در راستای بررسی شناسایی و رتبه‌بندی عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات، دو سؤال مطرح شد. سؤال اول این بود که چه عواملی بر موفقیت سامانه مدیریت یکپارچه تهدیدات تأثیرگذارند و سؤال دوم عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات را رتبه‌بندی می‌کرد. برای پاسخگوئی به سؤال‌ها، از آزمون تحلیل سلسله مراتبی فازی و رتبه‌بندی عوامل مؤثر بر موفقیت بر اساس روش تاپسیس استفاده شد.

نخست سؤال اول پژوهش تحت عنوان عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات، مورد بررسی قرار گرفت. بر اساس نتایج با استفاده از روش تحلیل سلسله مراتبی فازی چهار گروه عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات شناسایی شد. شواهد در پاسخ به سؤال اول پژوهش نشان داد که عوامل فردی، عوامل عملکردی، عوامل سازمانی و عوامل محیطی از مهمترین عوامل تأثیرگذار بر موفقیت سامانه مدیریت یکپارچه تهدیدات است. نتایج رتبه‌بندی تحلیل سلسله مراتبی فازی برای عوامل تأثیرگذار بر موفقیت سامانه مدیریت یکپارچه تهدیدات متفاوت است و میزان اهمیت آنها به این صورت است که عوامل فردی و عوامل عملکردی با وزن ۰/۲۵۵ بیشترین اهمیت را دارد و عوامل محیطی با وزن ۰/۲۴۳ کمترین رتبه یا اندازه را دارد. در مقایسه با پژوهش‌های پیشین نظر به اینکه تاکنون هیچ پژوهشی به بررسی عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات نپرداخته و این تحقیق نخستین پژوهشی است که این عوامل را مشخص می‌کند؛ لذا انجام مقایسه امکان‌پذیر نیست. پس نتایج این پژوهش می‌تواند زمینه‌ساز پژوهشهای آینده باشد. درخصوص پیشنهاد کاربردی باتوجه به رشد سریع در تولید محصول UTM و نیاز اساسی شبکه‌های رایانه‌ای به این محصول، به‌عنوان توصیه‌های اجرائی پیشنهاد می‌شود که دولت و شرکت‌های خصوصی برای تولید این محصول در داخل کشور برنامه ویژه‌ای تدوین کنند.

در پاسخ به سؤال دوم پژوهش، رتبه‌بندی عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات، مورد بررسی قرار گرفت. بر اساس نتایج با استفاده از روش تحلیل سلسله مراتبی فازی چهار گروه عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات در شرکت امن‌پرداز کویر شناسایی شد که عبارت است از: عوامل فردی، عوامل عملکردی، عوامل سازمانی، و عوامل محیطی که با استفاده از روش تاپسیس فازی، نتایج رتبه‌بندی شد. میزان اهمیت آنها به این صورت است که عوامل فردی و عوامل عملکردی با وزن ۰/۲۵۵ بیشترین اهمیت را دارد و عوامل محیطی با وزن ۰/۲۴۳ کمترین رتبه یا اندازه را دارد. نظر به اینکه تاکنون هیچ پژوهشی به بررسی عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات نپرداخته و این پژوهش نخستین پژوهشی است که این عوامل را رتبه‌بندی می‌کند؛ لذا انجام مقایسه امکان‌پذیر نیست؛ پس نتایج این پژوهش می‌تواند زمینه‌ساز پژوهشهای آینده باشد. درخصوص پیشنهاد کاربردی با توجه به رشد سریع در تولید محصول UTM و نیاز اساسی شبکه‌های رایانه‌ای به این محصول، به‌عنوان توصیه‌های اجرائی پیشنهاد می‌شود که دولت و شرکتهای خصوصی تدابیر و راهبردهای تولید این محصول را بر اساس اهمیت این محصول و رتبه‌بندی حاصل‌شده ارائه کنند. بدین‌صورت که عوامل فردی و عوامل عملکردی در صدر برنامه‌های راهبردی دولتمردان باشد.

رتبه‌بندی عوامل فردی بیشترین نمره را به خود اختصاص داده است؛ بر اساس آزمون فریدمن عامل مهارت با میانگین رتبه ۱۱/۱۳ اولین عامل در موفقیت سامانه مدیریت یکپارچه از بین عوامل فردی است. پس از آن به ترتیب مسئولیت‌پذیری با میانگین رتبه ۱۱/۱۲ دومین عامل فردی در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، صداقت و درستی اعضا با میانگین رتبه ۱۰/۶۰ سومین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، تجربه مدیر با میانگین رتبه ۱۰/۴۰ چهارمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، شهامت و شجاعت کارکنان با میانگین رتبه ۹/۰۷ پنجمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، اعتمادبه‌نفس با میانگین رتبه ۹/۰۵ ششمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، قدرت انعطاف‌پذیری با میانگین رتبه ۸/۰۹

هفتمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، ایده و تفکرات نوین مدیریت با میانگین رتبه ۶/۸۹ هشتمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، استقامت و پشتکار کارکنان با میانگین رتبه ۶/۹۱ نهمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، خلاقیت و نوآوری مدیران با میانگین رتبه ۶/۸۹ دهمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، رقابت‌پذیری مدیران در پذیریش رقبا با میانگین رتبه ۶/۸۳ یازدهمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، هوش و استعدادها با میانگین رتبه ۶/۶۲ دوازدهمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، تحصیلات دانشگاهی با میانگین رتبه ۶/۱۵ سیزدهمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، خطرپذیری کارکنان با میانگین رتبه ۵/۴۶ چهاردهمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی، فروتنی اعضا با میانگین رتبه ۴/۴۰ پانزدهمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل فردی است. چنانکه سازمان در راستای موفقیت سامانه مدیریت یکپارچه تهدیدات در عوامل فردی ضعف داشته باشد و بخواهد بر تقویت اعضا، کارکنان و مدیران سرمایه‌گذاری کند، باید بر عواملی مانند افزایش مهارت کارکنان، مسئولیت‌پذیری کارکنان، اعتمادبه‌نفس کارکنان، شهامت و شجاعت کارکنان، صداقت و درستی اعضا، فروتنی اعضا، استقامت و پشتکار کارکنان، قدرت انعطاف‌پذیری، تجربه مدیران، هوش و استعداد در بین کارکنان، تحصیلات دانشگاهی کارکنان، خطرپذیری کارکنان، رقابت‌پذیری مدیران در پذیرش رقیبان، خلاقیت و نوآوری مدیران و ایده و تفکرات نوین مدیران تأکید کند. هنگامی‌که اعضا، کارکنان و مدیران در موارد یادشده توانمند شدند، قطع یقین مطابق با شواهد این پژوهش، اعضا، کارکنان و مدیران در مجموعه و سازمان، در عوامل عملکردی که یکی از عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات است، مشکلی نخواهند داشت.

در بررسی عوامل عملکردی، انجام وظایف مدیران به نحو احسن با میانگین رتبه ۳/۴۹ اولین است. بر اساس شواهد آزمون فریدمن عامل عملکردی انجام وظایف مدیران به نحو احسن با میانگین

رتبه ۳/۴۹ اولین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل عملکردی است. پس از آن به‌ترتیب انجام وظایف هر یک از اعضا در سازمان به نحو احسن با رتبه ۳/۰۹ دومین عامل عملکردی در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل عملکردی، مدیریت زمان با میانگین رتبه ۲/۹۷ سومین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل عملکردی، تقسیم‌کار با میانگین رتبه ۲/۷۶ چهارمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل عملکردی، آینده‌نگری با میانگین رتبه ۲/۷۰ پنجمین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل عملکردی است. پس چنانکه سازمان در راستای موفقیت سامانه مدیریت یکپارچه تهدیدات در عوامل عملکردی ضعف داشته باشد و سازمان در نظر داشته باشد بر تقویت اعضا، کارکنان و مدیران در مجموعه و سازمان سرمایه‌گذاری کند، باید بر عواملی نظیر افزایش انجام وظایف مدیران به نحو احسن و انجام وظایف هریک از اعضا در سازمان به نحو احسن، آینده‌نگری اعضا در سازمان، مدیریت زمان در بین تمام مجموعه، و تقسیم‌کار اعضا تأکید کند. هنگامی‌که اعضا، کارکنان و مدیران در مجموعه و سازمان در موارد یادشده توانمند شدند، قطع یقین مطابق با شواهد این پژوهش، اعضا، کارکنان و مدیران در مجموعه و سازمان، در عوامل عملکردی که یکی از عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات است، مشکلی نخواهند داشت.

بر اسا شواهد آزمون فریدمن، ساختار سازمانی با میانگین رتبه ۴/۵۶ اولین عامل در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل سازمانی است. پس از آن به‌ترتیب اهداف سازمانی از پیش‌تعیین‌شده با رتبه ۴/۲۳ دومین عامل عملکردی در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل سازمانی، فرهنگ و جو سازمانی با رتبه ۴/۲۰ سومین عامل عملکردی در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل سازمانی، آموزشهای ضمن خدمت به اعضا در سازمان با رتبه ۴/۱۳ چهارمین عامل عملکردی در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل سازمانی، منابع سازمانی با رتبه ۴/۰۳ پنجمین عامل عملکردی در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل سازمانی، برنامه‌های انگیزشی در سازمان با رتبه ۳/۶۵ ششمین عامل عملکردی

در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل سازمانی و اختیار عمل اعضا با رتبه ۳/۲۰ هفتمین عامل عملکردی در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل سازمانی است. پس سازمان در راستای موفقیت سامانه مدیریت یکپارچه تهدیدات اگر در عوامل سازمانی ضعف داشته باشد و سازمان در نظر داشته باشد بر تقویت اعضا، کارکنان و مدیران در مجموعه و سازمان سرمایه‌گذاری کند، باید بر عواملی نظیر اختیار عمل اعضا، اهداف سازمانی از پیش تعیین‌شده، فرهنگ و جو سازمانی، ساختار سازمانی، منابع سازمانی، برنامه‌های انگیزشی در سازمان، و آموزشهای ضمن خدمت به اعضا در سازمان تأکید کند. هنگامی‌که اعضا، کارکنان و مدیران در مجموعه و سازمان در موارد یادشده توانمند شدند، قطع یقین مطابق با شواهد این پژوهش، اعضا، کارکنان و مدیران در مجموعه و سازمان، در عوامل سازمانی که یکی از عوامل مؤثر بر موفقیت سامانه مدیریت یکپارچه تهدیدات است، مشکلی نخواهند داشت.

در انتها بر اساس آزمون فریدمن استفاده از فناوری روز با میانگین رتبه ۳/۴۳ اولین عامل محیطی در موفقیت سامانه مدیریت یکپارچه تهدیدات است. به‌ترتیب رفتار و واکنش رقیبان با رتبه ۳/۳۳ دومین عامل محیطی در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل محیطی، عوامل اقتصادی با رتبه ۲/۹۹ سومین عامل محیطی در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل محیطی، رفتار و عوامل قانونی و سیاسی با رتبه ۲/۷۷ چهارمین عامل محیطی در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل محیطی، عوامل فرهنگی و سازمانی با رتبه ۲/۴۹ پنجمین عامل محیطی در موفقیت سامانه مدیریت یکپارچه تهدیدات از بین عوامل محیطی است. در پیشنهاد آخر اگر سازمان در راستای موفقیت سامانه مدیریت یکپارچه تهدیدات در عوامل محیطی ضعف داشته باشد و سازمان در نظر داشته باشد بر تقویت اعضا، کارکنان و مدیران در مجموعه و سازمان سرمایه‌گذاری کند، باید بر عواملی نظیر عوامل اقتصادی، عوامل فرهنگی و اجتماعی، عوامل قانونی و سیاسی، استفاده از فناوری روز و رفتار و واکنش رقیبان تأکید کند. هنگامی‌که اعضا، کارکنان و مدیران در مجموعه و سازمان در موارد یادشده توانمند شدند، قطع یقین مطابق با شواهد این پژوهش، اعضا، کارکنان و مدیران در مجموعه و سازمان، در عوامل محیطی که یکی از عوامل مؤثر بر موفقیت

سامانه مدیریت یکپارچه تهدیدات است، مشکلی نخواهند داشت. در پایان ذکر این نکته خالی از لطف نیست که اگر در هر سازمانی اعضا، کارکنان و مدیران در موارد یادشده توانمند شدند و سازمان از هر حیث در عوامل فردی، عوامل عملکردی، عوامل سازمانی، و عوامل محیطی مشکلی نداشت، سامانه مدیریت یکپارچه تهدیدات به‌صورت موفق، توانایی برخورد و آمادگی مبارزه با هرگونه تهدیدات اینترنتی احتمالی را خواهد داشت.

منابع

آفرین‌محمدزاده، مجید؛ حسن‌زاده، رضا (۱۳۹۷)، شناسایی و رتبه‌بندی عوامل موثر در پیاده‌سازی مدیریت زنجیره تأمین سبز با روش AHP فازی و TOPSIS فازی در صنعت برق. **تصمیم‌گیری و تحقیق در عملیات**، ۳ (۳): ۲۸۱ ـ ۳۰۱.

بازآیی، قاسمعلی (۱۳۹۱)، **ابزارهای فناوری اطلاعات و ارتباطات**، تهران: شهر آشوب.

باقری‌پبدنی، محمد؛ داودی، سید محمدرضا (۱۳۹۶)، شناسایی و رتبه‌بندی عوامل تأثیرگذار بر انتقال فناوری با استفاده از روش AHP فازی (بررسی موردی: شرکت فولاد مبارکه اصفهان)، **فصلنامه تخصصی پارک‌های علم و فناوری و مراکز رشد**، ۵۳: ۷۵ ـ ۸۰.

بخردی‌نسب، وحید؛ ژولانژاد، فاطمه (۱۳۹۶)، بررسی رفتار مدیر در برخورد با هزینه‌ها بر اساس رویکرد رتبه‌بندی شرکت‌ها با مکانیزم‌های حاکمیت شرکتی در تاپسیس فازی، **مهندسی مدیریت نوین**، ۶ (۱ و ۲): ۱۷ ـ ۳۷.

بخردی‌نسب، وحید؛ ژولانژاد، فاطمه (۱۳۹۸)، تاثیر کیفیت مدیریت ریسک بر نوسانات ضمنی اعلان سود، **پژوهش حسابداری**، ۹ (۴): ۲۷ ـ ۵۱.

حق‌شناس کاشانی، فریده؛ سعیدی، نیما (۱۳۹۰)، رتبه‌بندی عوامل موثر بر رقابت‌پذیری صنعت فرش کشور با روش تاپسیس فازی، **تحقیقات بازاریابی نوین**، ۱ (۱): ۱۲۷ ـ ۱۵۴.

خیری، سعید (۱۳۹۴)، شناسایی، تحلیل و رتبه‌بندی عوامل مؤثر کلیدی در پیاده‌سازی سامانه مدیریت امنیت اطلاعات در سازمان‌های حاکمیتی (مطالعه موردی: سازمان بنادر و دریانوردی)، **مجله صنعت حمل و نقل دریایی**، ۲(۳): ۳۶ ـ ۴۶.

صارمی، محمود (۱۳۸۵)، طراحی مبتنی بر بدیهیات ابزاری جهت فازبندی و استقرار سامانه تولیدی، **فصلنامه دانش مدیریت**، ۱۹ (۴): ۲۰ ـ ۲۷.

فرهودی، حمید؛ عبدی، بهنام؛ آقامحمدی، وحید (۱۳۹۴)، شناسایی و اولویت‌بندی عوامل حیاتی موفقیت سامانه‌های اطلاعاتی در شرکت ملی پخش فرآورده‌های نفتی ایران با رویکرد برنامه‌ریزی راهبردی. **فصلنامه علمی ـ ترویجی فرآیند نو**، ۱۰ (۵۲): ۲۲۹ ـ ۲۵۰.

کرمی، غلامرضا (۱۳۹۲)، بررسی برخی معیارهای کیفیت سود در چرخه تجاری، **فصلنامه بررسی‌های حسابداری و حسابرسی**، ۲۰ (۴): ۹۳ ـ ۱۱۲.

مظلومی، نادر (۱۳۹۰)، شناسایی و رتبه‌بندی عوامل مؤثر در کسب مزیت رقابتی شرکت‌های بیمه، **پژوهشنامه بیمه (صنعت بیمه)**، ۲۷(۲). (مسلسل ۱۰۶): ۸۱ ـ ۱۰۹.

Ambashta, Ajitabh., Momaya, K., 2002, "Competitiveness of Firms: Review of Theory, Frameworks and models", **Singapore Management Review**, Vol 26 (1), pp. 45-58

Bruno, A. V., Tyebjee, T.T. (1982). **The environment for entrepreneurship**. In Kent, c., Sexton, D., Vesper, K. (eds) The Encyclopedial of Entreoreneurship. Englewood cliffs, NJ.

ENISA. (2018) "**ENISA Threat Landscape Report 2017**", Final version. 1.0 ETL 2017, www.enisa.europa.eu.

Federal Office for Information Security (BSI). (2018) "**Register of current cyber threats and attacks**", BSI-CS 026, Version 2.0, https://www.allianz-fuer-cybersicherheit.de.

Granadillo, G. Dubus, S. Motzek, A. Garcia-Alfaro, J. Alvarez, E. Merialdo, M. Papillon, S. Debar, H. (2018). Dynamic risk management response system to handle cyber threats. **Future Generation Computer Systems**. Volume 83, Pages 535-552.

Hax, Arnold & Wilde, Dean, 1999, "the delta model: Adaptive Management for a Changing World", **Sloan Management Review**, 40(2), pp: 11-28.

Hax, Arnold & Wilde, Dean, 2002, "**the Delta Model- toward a Unified Framework of Strategy**", MIT Sloan School of management, Working paper, 4261-02, pp: 1-36.

Hooley, et al, 2003, "The Performance Impact of Marketing Resources", **Journal of Business Research**, Volume. 58(1), pp: 18-27

Karsak, E. E. & Ozogul, C. O. (2002). An integrated decision making approach for ERP system selection. **Expert Systems with Applications**,36(1), 660-667.

Lamine, E. Thabet, R. Dominik, A. Franck, B. Herve, F. Pingaud, H. (2020). BPRIM: An integrated framework for business process management and risk management. **Computers in Industry**. Volume 117, 103199.

Liu, S., Sandra, et al, 2003, "Market-oriented Organizations in an Emerging Economy, A Study of Missing Links", **Journal of Business Research**, Vol. 56, p: 481-491

McClelland, D. (1987), Characteristics of successful entrepreneur, **The Journal of crestive Behavior**, vol. 21 No3.

McGahan, Anita, M., Silverman, Brian, S, 2006, "Profitting from Technilogical Innovation by Others: The Effect of Competitor Patenting on Firm Value", **Research Policy**, 35(8), October, pp: 1222-1242

McGhan, A. M., 1999, "Competition, Strategy and Business Performance", **California Management Review**, 41 (3), pp: 74-101

Meinig, M. Sukmana, M. Torkura, K. Meinel, C. (2019). Holistic Strategy-Based Threat Model for Organizations. **Procedia Computer Science**. Volume 151, Pages 100-107.

Mintzberg, H., Waters, J. (1982). Tracking strategies in and entrepreneurial firm, **Academy of management Journal.**

Navas, J. Beltrán, M. (2019).Understanding and mitigating OpenID Connect threats. **Computers & Security**. Volume 84, Pages 1-16.

Tam, K. Salvador, M,. H. McAlpine, K. Basile, R. Matsugu, B. More, J. (2013). **Introduction to UTM (Unified Threat Management)**. UTM Security with Fortinet. Mastering FortiOS. 2013, Pages 3-34.

The Guardian. (2018) "**Facebook says Cambridge Analytica may have gained 37m more users' data**", https://www.theguardian.com.

Yeh C.H., Deng, H., 2006, "A Practical Approach to Fuzzy Utilities Comparison in Fuzzy Multi-Criteria Analysis", **International Journal of Approximate Reasoning**, 35 (2), pp: 179-194.