الگوی شناختی امنیت سایبری انسان‌محور

چکیده

تغییرات فناوری به تهدیدات و حملات امنیتی جدیدی منجر می‌شود که سناریوهای جدید و پیچیده امنیت سایبری را با داده‌هایی با حجم، سرعت و تنوع بالا و بردارهای مختلف حمله ایجاد می‌کنند که می‌توانند از مهارت‌های شناختی کاربران و حتی تحلیلگران امنیتی فراتر روند. در این زمینه، علوم شناختی می‌تواند ضمن ارتقای قابلیت‌ها و آمادگی‌های شناختی نیروی انسانی سایبری با الگوبرداری از فرایندهای شناختی انسانی و بهره‌گیری از آن‌ها در فناوری‌های سایبر شناختی به کاربران امنیت سایبری کمک کند تا سرعت، دقت و اطمینان واکنش‌ها، تصمیمات و اقدامات خود را در عملیات سایبری ارتقاء داده و باعث بهبود سطح امنیت سایبری سازمان شوند. پژوهش حاضر ازنظر هدف، کاربردی و به لحاظ روش توصیفی- تحلیل محتوا هست که به‌صورت کتابخانه‌ای اجراشده است. ازآنجاکه مطالعات مربوط با امنیت سایبری شناختی انسان‌محور بیشتر به‌صورت کیفی و بدون داده‌های کمی هست، روش فرا ترکیب به‌عنوان روشی مناسب برای به دست آوردن ترکیب جامع از امنیت شناختی به‌کاررفته است. در این تحقیق از الگوی هفت مرحله‌ای سندلوسکی و باروسو (۲۰۰۷) استفاده شد. مدل پیشنهادی شناختی از اجزای آگاهی وضعیتی[۱]، خودآگاهی[۲]، اوودا[۳] و انسان در حلقه[۴] تشکیل گردیده است که برای ایجاد فرایند خودکارسازی و آگاهی در اجرای وظایف شناختی تعریف‌شده، عامل انسانی را به‌عنوان محور اصلی در فرایندهای اعتبار سنجی و تصمیم‌گیری در نظر می‌گیرد. برازش مدل از طریق ارسال، جمع‌آوری و تجزیه تحلیل پرسشنامه به 20 نفر از خبرگان حوزه علوم سایبری و شناختی مورد تائید قرار گرفته است.

کلیدواژه: امنیت سایبری، امنیت شناختی سایبری، آگاهی وضعیتی، آمادگی شناختی.

1.مقدمه

امروزه فناوری‌های مدرن توانایی دستیابی و توزیع گسترده اطلاعات بسیار سریع را در اختیار ما قرار داده است. پویایی، ابهام، پیچیدگی و عدم قطعیت ناشی از دسترس‌پذیری بیشتر به اطلاعات، کاهش زمان تصمیم‌گیری و افزایش دقت سلاح‌های سایبری منجر به افزایش نیازهای شناختی و فشار روانی در حملات سایبری شده است. چشم‌اندازهای مربوط به امنیت سایبری در حوزه‌ی علوم شناختی، بخصوص در سیستم‌های پیچیده‌ای که با استفاده از فناوری‌هایی مانند رایانش ابری ، موبایل، اینترنت اشیاء و شبکه‌های اجتماعی که مقادیر زیادی اطلاعات تولید می‌کنند، راه‌حل‌هایی برای تقویت ظرفیت‌های عامل انسانی است. امروزه، ضروری است به‌طور علمی سهم علوم شناختی به ظرفیت‌های انسان تقویت‌شده[1]، برای انجام وظایف امنیت سایبری که نیاز به استفاده از مهارت‌های شناختی دارد، مورد تجزیه‌وتحلیل واقع شود. علوم شناختی می‌تواند در تقویت فرایندهای ادراک[2]، فهم[3] و تجسم[4] که بخشی از فرایند آگاهی وضعیتی و خودآموزی[5] انسان هستند کمک کند. مطالعه علمی میان‌رشته‌ای روانشناسی، علوم محاسباتی، زبان‌شناسی، فلسفه و علوم اعصاب برای درک کارکرد ذهن انسان به‌عنوان علوم شناختی تعریف‌شده است که ساختار، فرایند و عملکرد شناختی ذهن را بررسی می‌کند (فردنبرگ و گوردون سیلورمن،1391). این کاربرد درزمینه امنیت سایبری امکان ایجاد ارتباط بین رویه‌ها، اقدامات امنیتی، دانش تولیدشده توسط سیستم‌های رایانه‌ای، وبلاگ‌های امنیتی، بولتن‌های آسیب‌پذیری و تجربه متخصصان امنیتی را بر اساس وظایف روزانه را مهیا می‌سازد که درنهایت باعث تولید یک شناخت (آگاهی یا بینش) در مورد وضعیت امنیت سایبری می‌شود. همکاری بین انسان و ماشین، استفاده از روش‌های آماری، یادگیری ماشین و کلان داده می‌تواند باعث ارتقاء یا گسترش مهارت‌های شناختی متخصصان امنیت در مراکز فعالیت‌های امنیتی[6] یا تیم‌های پاسخگویی به حوادث امنیتی[7] برای استفاده از این راه‌حل‌های متمرکز بر فرایندهای امنیت سایبری شود.

در یک فرایند مناسب، کاربران سایبری باید آگاهی از وضعیت سایبری در سازمان را برای شناسایی و پیش‌بینی تهدیدها یا حملات امنیتی درک کنند تا بتوانند تصمیم و اقدام صحیح و متناسب را انجام دهند. برای دستیابی به این آگاهی وضعیتی، تحلیلگران باید مقادیر زیادی از داده‌ها را که به‌سرعت در حال جمع‌آوری و

---

[1] Augmented human
[2] Perception
[3] Comprehension
[4] Projection
[5] Self-learning
[6] SOC
[7] CSIRT

ذخیره شدن می‌باشند را پردازش کرده و آن‌ها را با متغیرهای زمانی و مکانی مرتبط کنند؛ اما می‌توان ادعا کرد که علیرغم این حجم انبوه داده‌ها، افراد با فقر دانش در تصمیم‌گیری روبرو هستند (مربان و دیگران،2008) زیرا این فعالیت نیاز به تمرکز و آمادگی‌های شناختی بالای تحلیلگر امنیت دارد که می‌تواند تحت تأثیر عوامل مختلفی فردی، محیطی و سازمانی مانند استرس بالا، میزان هشدار کاذب بالا، تجربه پایین، وظایف بدون ساختار، روش غیراستاندارد برای شناسایی و پاسخ به حملات، حجم بالایی از داده‌ها و اطلاعات، منابع اطلاعات نامشخص و عدم وجود معیارهای عملکردی از سوی تحلیلگران و مرکز عملیات امنیتی[1] قرار گیرد.

اگرچه فناوری، نقش غیرقابل‌انکاری در امنیت سایبری دارد، اما در فضای سایبر به‌عنوان یک اکوسیستم (متشکل از ابعاد فناوری، انسان و فرایند) انسان نقش اصلی را در پویایی این فضا در نقش‌های مختلف دارد. تحلیلگر امنیت می‌تواند با بهره‌گیری از امنیت شناختی، بر وضعیت امنیت سایبری سازمان تمرکز کند تا بتواند فرآیندهای امنیت سایبری را برای شناسایی و پاسخگویی به عوامل امنیتی بهبود بخشد. ازنظر مفهوم امنیت شناختی مبتنی بر استفاده از هوش مصنوعی و تجزیه‌وتحلیل داده‌ها برای تقویت عملیات امنیت سایبری در یک سازمان از طریق شناسایی الگوهای رفتاری است. بااین‌حال، سهم استفاده از سیستم‌های شناختی بیش از فرایند خودکار سازی (اتوماسیون) یا شناسایی الگوهای تهدیدات است و شامل تولید دانش لازم برای تصمیم‌گیری، تجزیه‌وتحلیل بلادرنگ تهدیدها و شبیه‌سازی تفکر انسان در فرایندهای شناختی امنیت سایبری است.

[1] SOC

1-1 بیان مسئله

فضای سایبر به‌عنوان یک زیست‌بوم (اکوسیستم) با ماهیت فناورانه- اجتماعی[1] دارای ابعاد فناوری، انسان (مدافع، مهاجم و کاربر) و فرایندها است (الصباغ،2017) و اکثر مدل‌های ارائه‌شده برای فضای سایبر مانند مدل‌های شلدون[2]، شاو[3]، کلارک[4]،ITU[5]، DOD[6]و مدل ارائه‌شده توسط مرکز ملی فضای مجازی نیز علاوه بر لایه‌های فیزیکی و اطلاعاتی دارای یک‌لایه شناختی، انسانی و یا اجتماعی هستند. بااین‌وجود بیشتر راه‌کارهای ارائه‌شده برای امنیت و دفاع از این فضا با رویکرد صرفاً فناورانه ارائه‌شده است. این راه‌کارها بیشتر به تقویت امنیت و دفاع از لایه‌های فیزیکی و اطلاعاتی فضای سایبر پرداخته و توجه کمتری به جنبه‌های شناختی کاربران و تحلیلگران و تصمیم‌گیرندگان داشته است، در حال که بسیاری از حملات سایبری ثبت‌شده با بهره‌گیری از محدودیت‌های شناختی عامل انسانی، راه‌حل‌های امنیتی صرفاً فناورانه را به‌طور مؤثر شکست داده‌اند.(لافوند و دوشارم،2012).

امنیت سایبری از تلاقی اطلاعات، فناوری، افراد و زمینه برای استخراج دانش در مورد آگاهی پویا و چگونگی ظهور آن در طول زمان در نظر گرفته می‌شود (مک نی و هال،2017). در حال حاضر حملات و تهدیدات پیشرفته مداوم[7] هوشمند به نقاط ضعف و آسیب‌پذیری‌ها، بیشتر به بخش کاربران تمرکز دارد و علی‌رغم پیشرفت‌های چشم‌گیر در بعد فناوری، شایستگی‌های تحلیلی تصمیم‌گیرنده انسانی، از طریق بهره‌برداری از فرآیندهای شناختی جهت مقابله با این تهدیدات، هنوز هم ناگزیر و ضروری هستند (برتون و روسو،2018). عدم شناسایی، حفظ و تقویت آمادگی‌های شناختی (دانش، مهارت، توانایی و نگرش) موردنیاز فرد برای ایجاد و حفظ کارایی و اثربخشی شایسته در محیط‌های پیچیده عملیات سایبری موجب بروز خطاها و سوگیری‌های شناختی و درنتیجه اخذ تصمیمات و اقدامات نامناسب دفاع سایبری شده است.

ظهور فناوری‌هایی مانند کلان داده، اینترنت اشیاء، رایانش ابری و کوانتومی، موبایل، روبات‌های خودمختار موجب تولید داده‌هایی با حجم، سرعت و تنوع بالا شده که افزایش پیچیدگی، پویایی و عدم قطعیت فضای سایبری را در پی داشته است. عدم بهره‌گیری مناسب و نظام‌مند از فناوری‌ها و سیستم‌های سایبر- شناختی (یادگیری ماشین، داده‌کاوی، پردازش زبان طبیعی و ...) برای داده‌کاوی، تجزیه‌وتحلیل داده‌ها، استخراج اطلاعات و کسب دانش برای پشتیبانی از تصمیم عامل انسانی در عملیات دفاع سایبری باعث ایجاد فضایی انباشته از

---

[1] Techno-social
[2] Sheldon
[3] Shaw
[4] Clarck
[5] International cominucation union
[6] Department of defence
[7] Advanced Persistence Threats

داده‌های ساختاریافته و ساختار نیافته، مبهم و همراه با عدم قطعیت شده است که علی‌رغم وجود حجم انبوهی از داده‌ها سازمان‌ها را با فقر دانش در تصمیم‌گیری روبرو کرده است.

از سوی دیگر به دلیل عدم وجود فرایندهای شناختی استاندارد (آگاهی از وضعیت، خودآگاهی، چرخه تصمیم‌گیری، یادگیری مولد و در لحظه و...) به‌عنوان حلقه اتصال فناوری و عامل انسانی امکان بهره‌گیری بهینه از ظرفیت‌های آن‌ها برای ایجاد هم‌افزایی در امنیت سایبری مقدور نبوده که این چالش باعث کاهش سرعت کشف، شناسایی و پاسخگویی به حملات و تهدیدات سایبری شده است. لذا نظر به اهمیت این بعد (شناختی) از امنیت سایبری نیاز به بررسی و ارائه مدلی از امنیت سایبری برای ادغام تئوری‌های شناختی با روش‌ها و مدل‌های به‌کاررفته درزمینه امنیت سایبر ضروری هست تا فرآیندهای تصمیم‌گیری افراد فعال در فضای سایبری را بهبود بخشد.

هدف این تحقیق مطالعه روش امنیت شناختی و شناسایی راه‌حل‌هایی با بهره‌گیری از علوم و فناوری‌های سایبر شناختی و چگونگی ادغام آن‌ها با فرآیندهای شناختی کاربران سایبری است که نتیجه آن می‌تواند برای درک، فهم، تولید دانش و اجرای اقدامات امنیتی استفاده شود. همچنین در این تحقیق فرآیندهای عملیات سایبری برای ایجاد فرایند خودکارسازی در اجرای وظایف شناختی و با در نظر گرفتن تحلیلگر (عامل انسانی) به‌عنوان محور اصلی در فرایندهای اعتبار سنجی و تصمیم‌گیری جهت ارائه یک مدل امنیت شناختی موردبررسی قرار می‌گیرد. این زمینه‌ها باعث تحقیق در دو موضوع جنبه‌های رفتاری و شناختی انسان در چارچوب عملیات امنیت سایبری و آگاهی (آگاهی از وضعیت و خودآگاهی) را برای درک اقدامات امنیتی، وظایف عملیاتی و دانش حاصل از وقایع امنیت سایبری فراهم می‌کند.

2- مبانی نظری پژوهش

2-1 پیشینه و مفهوم امنیت شناختی

ازنظر مفهوم امنیت شناختی مبتنی بر استفاده از هوش مصنوعی و تجزیه‌وتحلیل داده‌ها برای تقویت عملیات امنیت سایبری در یک سازمان از طریق شناسایی الگوهای رفتاری است. بااین‌حال، سهم استفاده از سیستم‌های شناختی بیش از فرایند خودکارسازی یا شناسایی الگو است و شامل تولید دانش برای تصمیم‌گیری، تجزیه‌وتحلیل بلادرنگ تهدیدها و شبیه‌سازی تفکر انسان در فرایندهای شناختی تجزیه‌وتحلیل امنیت است. امنیت شناختی توسط «تورس و آندراده»[1] به توانایی ایجاد شناخت برای تصمیم‌گیری کارآمد و بلادرنگ توسط انسان یا سیستم رایانه‌ای، بر اساس درک امنیت سایبری که سیستم رایانه‌ای از محیط خود (آگاهی از وضعیت) و دانش در مورد

[1] Torres & Andrade

خود (خودآگاهی یا بینش) اطلاق شده است (تورس و آندراده،2018). بنا به گفته شرکت سیسکو امنیت شناختی بر روی استفاده از هوش مصنوعی برای شناسایی تهدیدات پیشرفته امنیت سایبری از طریق تجزیه‌وتحلیل بلادرنگ داده‌ها متمرکزشده است (سیسکو،2018). از نگاهی دیگر با توجه به قابلیت‌های شناختی می‌توان آن را به استفاده از روش‌های غیر فنی برای کاهش آسیب‌پذیری افراد در معرض دست‌کاری ادراک انسانی که به‌عنوان هک شناختی شناخته می‌شود اطلاق نمود که از راه‌حل‌های فنی نیز برای تشخیص داده‌های گمراه‌کننده و اطلاعات غلط و جلوگیری از انتشار آن‌ها، استفاده می‌کند (رز،2017). به عقیده شرکت IBM سیستم‌های امنیت شناختی، سیستم‌های خودآموزی هستند که از داده‌کاوی، یادگیری ماشین، پردازش زبان طبیعی و تعامل انسان و رایانه برای شبیه‌سازی رفتار انسان استفاده می‌کنند. این کار بر اساس استفاده از سیستم‌های شناختی برای تجزیه‌وتحلیل روندهای امنیتی و چکیده‌سازی حجم عظیمی از داده‌های ساختاریافته و غیر ساختاری و تبدیل آن‌ها به دانش عملی برای ایجاد امنیت مستمر و پیشرفت‌های تجاری است (IBM،2017). موسسه NIST نیز با رویکردی تعاملی بین ماشین و انسان، امنیت شناختی را استفاده از ماشین‌آلات یادگیری برای درک کل اطلاعات مربوط به یک وضعیت، افزایش شناخت انسان به‌منظور کمک به آن‌ها در تصمیم‌گیری مؤثرتر در نظر می‌گیرد (NIST،2016). از دیدگاه «ملور[1]» امنیت شناختی بر یادگیری مداوم برای افزایش دانش یک سیستم امنیتی است که ناهنجاری‌های رفتاری را شناسایی می‌کند و قادر است با استفاده از هوش مصنوعی موضوع را ارزیابی کند و فرضیه‌های خودش را بگیرد، تحلیلگران وظایف را از تعریف قوانین سخت‌گیرانه یا تله‌های امنیتی رها کند و می‌تواند بینشی فراهم کند که بسیار سریع‌تر از انسان‌های تیزهوش باشد (ملور،2018).«فورد و سراجی»[2] با نگرشی فناورانه امنیت شناختی را به‌عنوان تولید دانش از الگوهایی که به‌عنوان نرمال شناخته می‌شوند و از طریق حسگر و داده‌های تحلیلی متغیرهای خود سیستم و محیط آن به دست می‌آیند تلقی کرده که سطح مشخصی از هوش را به سیستم‌های رایانه‌ای ارائه می‌دهد (فورد و سراجی،2014).

به‌طورکلی می‌توان گفت امنیت شناختی از طریق تجزیه‌وتحلیل داده‌ها (کلان داده‌ها، فرآیندهای تصادفی، نظریه بازی) و با استفاده از تکنیک‌های هوش مصنوعی (یادگیری ماشین، پردازش زبان طبیعی و تعامل انسان و رایانه) فرایند تفکر ، یادگیری مداوم، تصمیم‌گیری و تجزیه‌وتحلیل امنیت را از فرایندهای شناختی انسان تقلید می‌کند.

[1] Melore
[2] Ford & Siraj

2-2 علوم شناختی

علوم شناختی به‌عنوان یکی از دانش‌های نوین در سال‌های اخیر توسعه فراوانی یافته است، به‌طوری‌که پیش‌بینی می‌شود با کمک سایر دانش‌های جدید ازجمله فن‌آوری زیستی[1]، علم کامپیوتر و فن‌آوری اطلاعات[2] و فن‌آوری نانو[3] تحول عمیقی در زندگی بشر ایجاد کند (وارلاو دیگران،2017). علم شناختی مطالعه علمی و بین‌رشته‌ای ذهن و فرآیندهای آن است که ساختار، فرایند و عملکرد شناختی ذهن را بررسی می‌کند و علوم شناختی دارای زیرشاخه‌های مدل‌سازی شناختی، روانشناسی شناختی، علوم اعصاب شناختی[4]، زبان‌شناسی شناختی[5]، فلسفه ذهن[6] و هوش مصنوعی است. مطالعات هوش، یادگیری، تفکر و حافظه نیز در حوزه علوم شناختی مطرح است. همچنین دانشمندان این حوزه در مورد چگونگی فعالیت سیستم‌های عصبی، ارتباط آن با ذهن و ارگانیسم، پردازش اطلاعات و چگونگی فرایند یادگیری نیز مطالعه می‌کنند (میلر،2003). علوم شناختی با تسلط بر سازوکارهای مغز برای یادگیری، یادسپاری، تفکر، بازنگری و تسلط بر ذهن افراد می‌تواند راهکارهایی برای تأثیرگذاری بر ذهن دیگران و تغییر، اصلاح یا تقویت آن پیشنهاد کند. وظیفه علم شناختی تجزیه‌وتحلیل شناختی است، ابزاری که بسیاری از سازمان‌ها، از آن در جهت یادگیری و تصمیم‌گیری استفاده می‌کنند (کاویانی و دیگران،2009). علوم شناختی به‌واسطه‌ی تأثیرگذاری و پیدایش فضای سایبر اعتبار و مصداق خاصی پیداکرده است و این دو تأثیر و تأثر زیادی بر یکدیگر دارند.

3-2 آگاهی وضعیتی سایبری[7]

مفهوم آگاهی از وضعیت، وضعیت فعلی سازمان را در مورد تهدیدها و حملات، تأثیر یک حمله احتمالی و شناسایی مهاجم و رفتار کاربر شرح می‌دهد (تیمنون،2015). همه این‌ها امکان پیش‌بینی وضعیت سازمان را در آینده نزدیک فراهم می‌کنند (اسکات و ربه‌کا،2017). درزمینه امنیت سایبری، آگاهی از وضعیت در سه سطح تعریف‌شده است:

1. درک[8]، توسط اطلاعات عناصر موجود در فضای سایبری مانند فایروال، SIEM[9] یا اخبار امنیتی تولید می‌شود.

---

[1] Biotechnology
[2] Computer science and Information technology
[3] Nanotechnology
[4] Cognitive neuroscience
[5] linguistics Cognitive
[6] Philosophy of mind
[7] Cybersecurity situation awareness
[8] Perception
[9] Security information and event managment

2. فهم[1]، وضعیت فعلی موقعیت را بر اساس تجزیه‌وتحلیل حمله مبتنی بر سطح تهدید یا خطر تعیین می‌کند.

3. تجسم و پیش‌بینی[2]، پیش‌بینی نوع آسیب‌پذیری‌ها، تهدیدها یا حملات را ایجاد می‌کند (توماس و منز،2017).

در حوزه نظامی، خلبانان نیروی هوایی ایالات‌متحده آمریکا بر اساس چهار مرحله حلقه OODA که توسط جان بوید پیشنهادشده بود، آگاهی از وضعیت را به دست می‌آوردند. پیشنهاد OODA مبتنی بر مشاهده و فهم محیط برای روند تصمیم‌گیری است. دو جنبه مهم حلقه OODA محدودیت زمانی و عدم قطعیت اطلاعات است (برتون و روسو،2018). تحلیلگر باید وضعیت امنیتی را درک و احتمال تأثیرگذاری را مشخص کند.

2-4-1 آگاهی وضعیتی سایبر شناختی[3](CCSA)

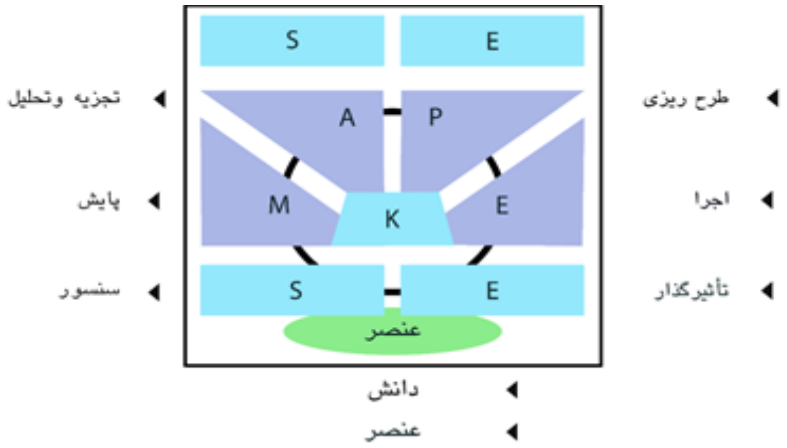
آگاهی وضعیت سایبری صرفاً نتیجه یک فرآیند فناورانه نیست، زیرا خروجی یک سیستم اجتماعی- فنی است که در آن انسان نقش اساسی را ایفا می‌کند. توانایی فناوری برای تفکر نقادانه و نتیجه‌گیری و اتخاذ تصمیمات و نتیجه‌گیری‌های شهودی متضاد در مواجهه با دشمن (شروع‌کننده یک نفوذ) پیش‌بینی‌نشده، محدود است؛ بنابراین وجود انسان در حلقه امنیت سایبری هنوز ضروری است. سطوح شناختی بالاتر مانند شهود، قضاوت، بداهه گویی و تجسم و به‌ویژه در توسعه خلاقانه استراتژی‌های حل مسئله ضروری هستند (موری،2016). تجزیه‌وتحلیل کارکردهای اجرایی فرآیندهای شناختی ادراک، فهم و تجسم در مدل مدیریت امنیت سایبری مبتنی بر آگاهی وضعیتی می‌تواند فرآیند تصمیم‌گیری و عملکرد تیم‌های سایبری را ارتقاء دهد. جنبه‌های مختلفی وجود دارد که مهارت‌های شناختی نقش مهمی ایفا می‌کنند، زیرا بدون ارتباطات کافی و توانایی اشتراک‌گذاری دانش، تیم‌های امنیت سایبری کارایی لازم برای مقابله با حملات امنیتی را نخواهند داشت (میمیر و دیگران،2015). برای ایجاد آگاهی از وضعیت امنیت سایبری سازمان، می‌توان از جنبه‌های شناختی برای پشتیبانی از فرآیندهای تصمیم‌گیری بهره برد.

2-4 خودآگاهی[4]

آگاهی، مفهومی از حوزه روانشناسی است که به‌عنوان ظرفیت انسان برای ایجاد فهم در مورد زندگی خود، بر اساس تجربه‌هایش تعریف‌شده است (بیکر،1987). این مفهوم توسط بسیاری از محققان در حوزه‌ی مهندسی و

[1] Comprehension
[2] Projection
[3] Cyber-cognitive situation awareness
[4] Self Awareness

سیستم‌های رایانه‌ای تطبیق یافته است، به‌عنوان‌مثال لوئیس[1] و همکاران، خودآگاهی از یک سیستم محاسباتی را توانایی دستیابی به دانش درباره خود، مبتنی بر وقایع داخلی و خارجی تعریف می‌کند (لوییس و دیگران،2016). در کار تحقیقی کامارا[2]، خودآگاهی[3] به‌عنوان ظرفیت استقلال، ظرفیت اجتماعی و فعالیتی که یک سیستم رایانه‌ای می‌تواند برای تولید دانش در مورد خود و محیط خود و تعیین فعالیت‌هایی که طبق آن دانش اجراشده، تعریف گردیده است (کامارا و دیگران،2017).در سال 2001، IBM تکنیکی را مبتنی بر کنترل بازخورد برای سیستم‌های رایانه‌ای معروف به MAPE-K ارائه داد (آموند و رودوس،2016).



شکل 1. مدل رایانش خودمختار سایبرنتیک

پنج مرحله MAPE-K شامل نظارت[4]، تحلیل[5]، طرح‌ریزی[6]، اجرا[7] و دانش[8] است. بر مبنای این مدل، مدل دیگری به نام مدل «رایانش خودمختار سایبرنتیک»[9] توسط فرد[10] و همکاران ارائه گردید. این طرح بر اساس مقدماتی بناشده که بتواند در تمام سطوح انتزاعی، عناصر سیستم را سنجش، تصمیم‌گیری و کنترل کند. به این حلقه کنترل، «رایانش خودمختار» گفته می‌شود. حلقه‌های کنترل برای ایجاد قابلیت «خود پیکربندی»[11]، «خود

[1] Lewis
[2] Camara
[3] Self -awareness
[4] Minitor
[5] Analyze
[6] PLAN
[7] Execute
[8] Knowledge
[9] Autonomic Computing Cybernetics
[10] Fered
[11] Self -configuring

ترمیمی»[1]، «خود بهینه‌سازی»[2] و «خود محافظتی»[3] طراحی‌شده‌اند. شکل 1 ترکیب اجزای حلقه کنترل رایانش خودمختار را نشان می‌دهد (میمیر و دیگران،2015).

2-5 مهارت‌ها و آمادگی‌های شناختی در امنیت سایبری

تحلیلگر امنیت سایبری، تجربیات و دانش عملی را برای ارزیابی و تفسیر مشاهدات ادغام می‌کند تا فرضیه‌هایی را در مورد وقایعی که ممکن است حملات احتمالی باشند ایجاد نماید. برای این کار، باید چندین منبع داده و اطلاعات پردازش شود و همبستگی بین آن‌ها و محیط گرافیکی برقرار شود.

در سال 2017، آی.بی.ام[4] وظایف شناختی یک تحلیلگر امنیتی را در جریان تحقیقات یک حادثه امنیتی ارائه داد که به شرح زیر است:

1. شناسایی؛ (مرور داده‌های حادثه، بازنگری رویدادها با در نظر گرفتن جنبه‌های منافع سازمان)
2. مشاهده؛ (رسم محوری در داده‌ها برای یافتن مقادیر غیرعادی یا نامتجانس، بسط جستجو برای یافتن اطلاعات بیشتر).
3. تولید فرضیه؛ (بررسی تهدیدات برای توسعه تجربه، کشف تهدیدهای جدید، تعیین شاخص‌های تعهد در منابع دیگر).
4. تحقیق در مورد فرضیه؛ (استفاده از اطلاعات برای تحقیق در مورد این حادثه، کشف آی.پی‌های آلوده احتمالی، تعیین حادثه بر اساس دانش تولیدشده‌ی مربوط به بررسی تهدید، تجزیه‌وتحلیل بر اساس مشخصات حمله،)(آی.بی.ام،2017).

در سطوح مختلف امنیت سایبری، نقش انسان عامل مهمی است که تنها با اجرای راهکارهای خودکارسازی نمی‌توان نقش آن را کاهش و یا حذف کرد، بلکه راه‌حل در تقویت آمادگی‌های شناختی عامل انسانی است. در توسعه مفهوم آمادگی شناختی، نویسندگان بر لزوم به‌کارگیری در فضای نبردهای مدرن (مانند فضای سایبری) که فضایی پیچیده، پویا و دارای منابع محدود است، تأکید کرده‌اند (اتر و دیگران،2000). مفهوم این امر این است که تحلیل گران سایبری باید ازنظر ذهنی آماده باشند تا عملکرد خود را در مواجهه با عوامل استرس‌زا، مانند فشار بیش‌ازحد اطلاعات، عدم اطمینان اطلاعات، انزوای اجتماعی، خستگی، ناراحتی جسمی و خطر، حفظ کنند. این

[1] Self -healing
[2] Self -optimizing
[3] Self -protecting
[4] IBM

امر مستلزم انعطاف‌پذیری و حتی خلاقیت در پاسخگویی به چالش‌های ناشی از پیچیدگی، پویایی و عدم قطعیت فضای سایبر است. با توجه به این پیش‌زمینه، تعریف زیر توسط فلچر[1] ارائه‌شده است:

«آمادگی شناختی، آمادگی ذهنی (شامل مهارت‌ها، دانش، توانایی‌ها، انگیزه‌ها و تمایلات شخصی) است که فرد برای ایجاد و حفظ عملکرد شایسته در محیط پیچیده و غیرقابل‌پیش‌بینی مدرن نیاز دارد». فلچر آمادگی شناختی را شامل 10 مؤلفه، «آگاهی از وضعیت، حافظه، انتقال آموزش، فراشناخت، خودکار بودن، حل مسئله، تصمیم‌گیری، انعطاف‌پذیری ذهنی، خلاقیت، رهبری و هیجان»[2] معرفی می‌کند (فلچر،2015). مؤلفه‌های آمادگی شناختی تحلیل‌گر سایبری را می‌توان به‌عنوان ترکیبی از سه توانایی اساسی زیر تقسیم کرد:

1. تشخیص الگوهای تهدیدات سایبری در موقعیت‌های آشفته و عدم قطعیت (آگاهی از وضعیت، حافظه، انتقال آموزش).
2. تطبیق و اصلاح راه‌حل‌های مرتبط با این الگوها، طبق شرایط موجود (فراشناخت، انعطاف‌پذیری، حل مسئله و خلاقیت)
3. اجرای برنامه‌های عملیاتی مبتنی بر این راه‌حل‌ها (تصمیم‌گیری، رهبری، خودکار بودن و کنترل احساسات).

ارتقاء آمادگی‌های شناختی تحلیلگران امنیتی، از طریق بهره‌گیری از روانشناسی، هوش مصنوعی، زبان‌شناسی و تعامل رایانه با انسان می‌تواند، زمان پاسخ و اثربخشی تصمیم‌گیری در مورد اقدامات تشخیص، مهار یا کاهش یک حمله امنیتی را بهبود بخشد.

2-6 فرایندها و وظایف شناختی برای آگاهی از وضعیت سایبری

مدل امنیتی شناختی، تحلیلگر امنیت را محور اصلی و اثربخشی آن بر خودکارسازی وظایف شناختی در امنیت سایبر اساسی می‌داند. مطابق مدل اوودا عناصر ایجادشده از ویژگی‌های شناختی برای فرآیندها، وظایف و مهارت‌های تحلیلگر امنیتی در چهار مرحله ایجاد می‌شود:

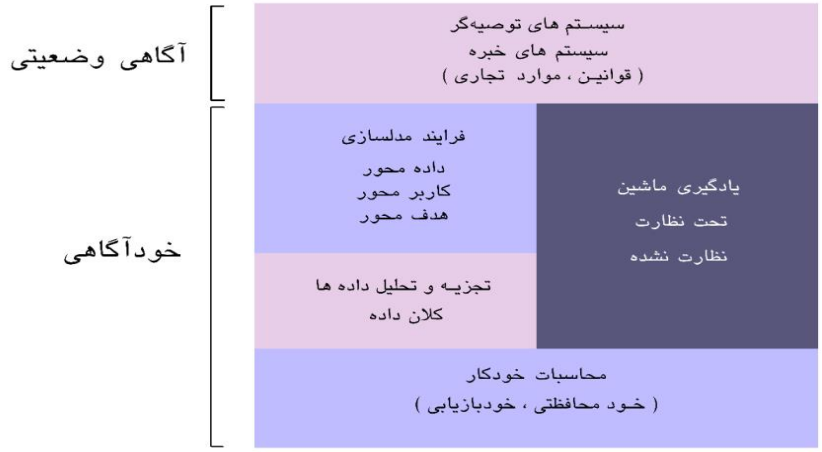
- مشاهده[3]؛ فرایند جمع‌آوری داده‌ها.
- جهت‌گیری[4]؛ ادغام اطلاعات برای ایجاد آگاهی از وضعیت.
- تصمیم‌گیری[1]؛ فرایند تصمیم‌گیری نهایی بر اساس تحلیل همه فرضیه‌ها.

---

[1] Feletcher
[2] Situation Awareness. Memory. Transfer of Training. Metacognition. Automaticity. Problem Solving. Decision-Making. MentalFlexibility. Creativity. Leadership. Emotion.
[3] Observation
[4] Orientation

- اقدام[2]؛ فرایند استدلال تحلیلی را تعریف می‌کند.

بر اساس تجزیه‌وتحلیل مفاهیم امنیت شناختی، نتیجه می‌گیریم که برای دستیابی به استفاده از شناخت در امنیت سایبری، مجموعه‌ای از راه‌حل‌های فنی و غیر فنی موردنیاز است. این مجموعه از مؤلفه‌ها باید با مدل امنیت شناختی و دو پارامتر تعریف‌شده درزمینه روانشناسی، خودآگاهی و آگاهی از وضعیت، سازگار باشند (تورس،2018) (شکل 2).



شکل 2. سطوح امنیت شناختی

اولین پارامتر شناختی که باید در امنیت شناختی ایجاد شود، خودآگاهی است. این پارامتر را می‌توان از طریق تعامل سیستم محاسباتی با سیستم‌های محیطی خود، مانند تعامل با سایر سیستم‌های رایانه‌ای، رفتار کاربران با سیستم رایانه‌ای، رفتار مهاجمان علیه سیستم رایانه‌ای، الگوهای داده، تجزیه‌وتحلیل درگاه‌های استفاده‌شده، تشخیص حالت‌های محاسباتی، تعامل کاربر و ماشین، تجزیه‌وتحلیل الگوهای زبان و حتی تصاویر به دست آورد (تورس،2018).

پارامتر بعدی آگاهی وضعیتی سایبری است که به سازمان‌ها این امکان را می‌دهد تا وضعیت فعلی خود را در رابطه با امنیت سایبری مانند مخاطرات، آسیب‌پذیری‌ها، حملات و شکاف‌ها مشخص کنند، بر اساس این دانش، سازمان‌ها می‌توانند وضعیت آینده خود را پیش‌بینی و تجسم نمایند. دو سطح ممکن برای آگاهی وضعیتی امنیت سایبری وجود دارد:

- سطح پایین که داده‌های خام پردازش می‌شود و متداول‌ترین روش برای یافتن راه‌حل‌های فناوری است که امکان خودکارسازی آن را فراهم می‌کند.

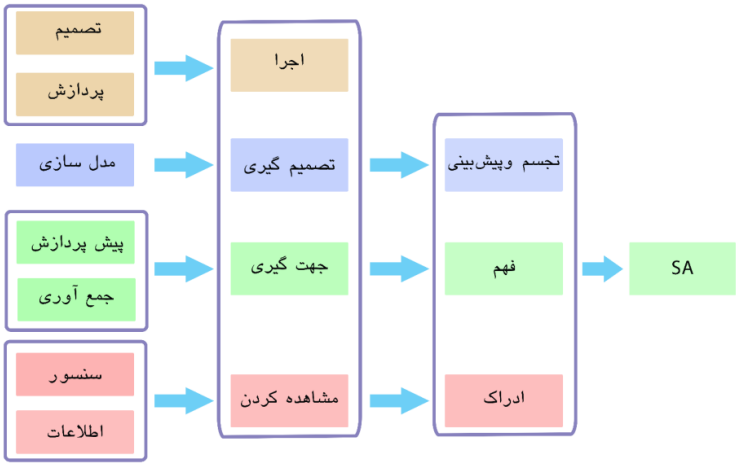
---

[1] Decision
[2] Action

- سطح بالایی که امکان ایجاد تصمیمات راهبردی را بر اساس فرآیندهای چکیده کردن اطلاعات فراهم می‌کند (پینو و دیگران،2014).

سطوح بالای آگاهی از وضعیت، معمولاً توسط انسان انجام می‌شود، این کار توان‌فرسا، وقت‌گیر و مستعد خطا است. راه‌حل‌های فنی درزمینه امنیت سایبری که می‌تواند توانایی‌های شناختی تحلیلگر امنیتی را برای ایجاد راهبردهای امنیت محرک تقویت کند، در زمینه‌های مختلف مانند تجسم سازی[1] برای امنیت سایبری، هوش مصنوعی یا کلان داده در امنیت سایبر توزیع می‌شود. امنیت شناختی منابع مختلف اطلاعات را برای ایجاد آگاهی از وضعیت در نظر می‌گیرد (اسکات و ربه‌کا،2017).

مقدار اطلاعات ممکن است از توانایی‌های تحلیل متخصصان امنیتی فراتر رود که برای آن‌ها استفاده از سیستم‌های پیشنهاد[2] یا سیستم‌های پشتیبانی از تصمیم خبره[3] می‌تواند فرایندهای تصمیم‌گیری را پشتیبانی کند. در مورد مدیریت شاخص‌های امنیت اطلاعات تحت یک مدل امنیتی شناختی مدلی توسط آندراده[4] ارائه‌شده که از هفت لایه تشکیل‌شده است. این مدل از راه‌حل‌های مختلف که می‌تواند مهارت‌های شناختی تحلیلگر امنیتی را تقویت کند، تشکیل‌شده است (آندراده و یو،2018).



شکل 3. فرایندها و وظایف شناختی برای آگاهی از وضعیت سایبری

[1] Visualization
[2] Recommendation Systems (RS)
[3] expert Decision Support Systems (DSS)
[4] Andrade

مدل فوق با استفاده از حلقه اوددا، الگوهای مشخص‌شده از طریق تجزیه‌وتحلیل داده‌ها را برای تولید مدل‌های ذهنی (بر مبنای پروفایل‌های حملات، تهدیدها، رفتار کاربران و مهاجمین) و ایجاد آگاهی از وضعیت سازمان به کار می‌برد و پس‌ازآن اقدامات طرح‌ریزی برای حفظ وضعیت امنیت سایبری را مشخص می‌نماید.

3- روش تحقیق

پژوهش‌های انجام‌شده درزمینه مدل شناختی امنیت سایبری انسان محورنشان داد که این پدیده موضوعی چندوجهی و پیچیده است، به‌گونه‌ای که اتفاق‌نظر در مورد ابعاد و عناصر آن وجود ندارد. به‌منظور درک بهتر موضوع موردمطالعه ازیک‌طرف و تنوع مفاهیم مرتبط با پدیده موردمطالعه لازم است که به یک درک و فهم مشترکی از مفاهیم مرتبط دست‌یابیم. تحقق این امر منوط به استفاده از رویکرد پژوهش کیفی است. این پژوهش در سه مرحله انجام می‌شود . در مرحله اول پژوهش ازآنجاکه هدف این پژوهش مطالعه موضوع قابلیت‌های شناختی عامل انسانی در امنیت سایبری است و برای این منظور نیاز به داده‌های کیفی وجود داشت، ابتدا پیشینه نظری و مفاهیم در حوزه‌های سایبری و شناختی و همچنین بررسی پیشینه تجربی و تحقیقات مرتبط موردتوجه قرار گرفت. در مرحله دوم از روش فراترکیب استفاده شده است. فراترکیب خانواده‌ای از رویکردهای روش‌شناختی برای توسعه دانش جدید بر پایه تحلیل دقیق و جامع یافته‌های تحقیق کیفی موجود است . در این روش پژوهشگر داده‌های ثانویه نتایج حاصل از سایر مطالعات را برای پاسخگویی به نتایج خود ترکیب نموده و نتایج جدیدی را به دست می‌آورد . در این مرحله الگوی هفت مرحله‌ای سندلوسکی و باروسو (۲۰۰۷) شامل:

۱)مشخص کردن هدف تحقیق ۲)جست‌وجوی نظام‌مند ادبیات پژوهش ۳) جست‌وجو و بررسی مقالات مرتبط ۴) استخراج اطلاعات مقالات ۵) تجزیه‌وتحلیل یافته‌های کیفی ۶) کنترل کیفیت ۷) ارائه یافته‌ها استفاده شد.

هدف پژوهش در روش فرا ترکیب بر اساس پارامترهایی چون چه چیزی، چه کسی «پایگاه‌های اطلاعات و مجلات معتبر»، چه زمانی (بازه زمانی ۲۰۰۰ تا 2022) و چگونه (شناسایی و یادداشت‌برداری نکات کلیدی، تحلیل مفاهیم و دسته‌بندی مفاهیم و مقوله‌ها) تعیین گردید. برای جست‌وجو در پایگاه داده‌ها، مجلات تخصصی، موتورهای جست‌وجو و همچنین پایگاه‌های فارسی از واژگان کلیدی با توجه به سؤالات پژوهش استفاده شد؛ که در جدول زیر آمده است. در این مرحله محقق با استفاده از کلیدواژه مطرح شده در جدول زیر در پایگاه داده Irandoc، Science Direct ,ISC, Scopus و همچنین پایگاه تخصصیscholarGoogle مقالات مرتبط را موردبررسی قرار داد.

واژگان کلیدی مورد جست‌وجو فارسی و انگلیسی امنیت سایبری، امنیت شناختی سایبری، خودآگاهی، آگاهی وضعیتی، آگاهی وضعیتی سایبری بوده است. در گام بعدی پژوهشگر به انتخاب مقالات و متونی پرداخته است که در راستای اهداف و سؤالات پژوهش است به‌محض این‌که مقالات متناسب با پارامترهای مطالعه بررسی شدند، قدم

بعدی ارزیابی کیفت روش‌شناختی مطالعات در دستور کار قرار گرفت. ابـزاری کـه در ایـن پـژوهش بـرای ارزیـابی مقالات کیفی مورد استفاده قرار گرفت، برنامه مهارت ارزیابی حیاتی[1] (CASP) است که بـا طـرح ده سـؤال بـه مـا کمک می‌کند تا دقت، اعتبار، اهمیت مطالعات کیفی پژوهش را مشخص کنیم. (مانیان، موسی خـانی، حسـن‌زاده و جامی پور، ۱۳۹۳).

در این مرحله پژوهش‌گر منابع منتخب را با توجه به موارد ده‌گانه بر اساس مقیاس ۵۰ امتیازی روبریک، سیسـتم امتیازبندی زیر را به کار گرفت: مقاله عالی (۵۰-۴۱)، خیلی خوب (۴۰ -۳۱)، متوسـط (۳۰-۲۱) و ضـعیف (۱۰ - ۰) (عرب و همکاران، ۱۳۹۳). مقالاتی که در سطح عالی و خیلـی خـوب مـورد ارزیـابی قـرار گرفتنـد، در تحلیـل مورداستفاده قرارگرفته‌اند.

در گام بعدی به‌منظور اطمینان از قابل‌قبول بودن و با هدف افزایش دقت ارزیـابی مقـالات منتخـب از روش چـک کردن به‌وسیله مشارکت‌کنندگان استفاده شده برای این کار مقالات در اختیار کارشناسان حوزه مربوطه قرار گرفت و آن‌ها بر اساس چک‌لیست CASP مقالات منتخب را مورد ارزیابی قرار دادند سپس نتایج حاصل از طریق ضـریب توافق کدگذاران با استفاده از شاخص کاپا و با کمـک نـرم‌افـزارSPSS مـورد تحلیـل قـرار گرفـت. در گـام بعـدی استخراج اطلاعات از منابع منتخـب و درنهایـت کدگـذاری بـاز و محـوری موردتوجـه قـرار گرفـت کـه در بخـش تجزیه‌وتحلیل داده‌های کیفی به آن اشاره گردید. حاصل کدگذاری باز و محوری شناسایی اولیه ابعاد و مؤلفـه‌هـای شناختی نیروی انسانی در امنیت سایبری است.

در مرحله دوم با استفاده از مصاحبه با خبرگان و متخصصان خواسته شد نظرات خود را درباره ابعاد و مؤلفـه‌هـای آمادگی شناختی در امنیت سایبری مطرح کنند بدون اینکه نتیجه تحقیق اولیه بـه آن‌هـا عرضـه شـود. بـه‌منظـور نمونه‌گیری و انتخاب خبرگان از روش نمونه‌گیری غیر احتمالی (روش گلوله برفی) استفاده شد، بدین‌صورت کـه از میان متخصصان و صاحب‌نظران موضوع علوم شناختی و امنیت سایبر، افرادی که با موضـوع موردمطالعـه آشـنایی نزدیکی داشتند، انتخاب شدند. البته تعداد متخصصان از قبل مشخص نبود، بلکه فرایند انجام مصاحبه تـا رسـیدن به حالت اشباع نظری ادامه پیدا کرد. بر اساس نظرات خبرگان الگوی اولیه را تکمیل و اصلاح گردید.

برای اعتبار یابی مدل به‌دست‌آمده آن را در اختیار 20 نفر از متخصصان و خبرگان قـرار داده و از آن‌هـا خواسـته شد نظرات خود را درباره اجزا و روابط مدل انیت شناختی سایبری و همچنین نظرات اصلاحی مطرح کنند.

3-1 جامعه آماری

[1] Critical Appraisal Skills program (CASP)

جامعه آماری این پژوهش در بخش فرا ترکیب مقالات و منابع پژوهشی مرتبط با ابعاد شناختی عامل انسانی در امنیت سایبری هستند که در ابتدا 50 مقاله مرتبط با امنیت سایبری، آگاهی وضعیتی سایبری و آگاهی وضعیتی سایبر شناختی شناسایی شدند و با استفاده از چک‌لیست ارزیابی حیاتی 30 مقاله برای تجزیه‌وتحلیل انتخاب شدند و در بخش مصاحبه و اعتباریابی الگوی امنیت شناخی سایبری، جامعه آماری پژوهش متخصصان و خبرگانی بوده است که در ارتباط با موضوع دارای سابقه علمی بودند و با موضوع موردمطالعه آشنایی داشتند.

3-2 حجم نمونه

به‌منظور انجام نمونه‌گیری از روش نمونه‌گیری نظری (غیر احتمالی) و هدفمند به روش گلوله برفی استفاده شد. بدین‌صورت که از میان متخصصان و صاحب‌نظران که با موضوع موردمطالعه آشنایی نزدیکی داشتند، به‌عنوان مصاحبه‌شونده انتخاب شدند. افراد بعدی با پیشنهاد همان صاحب‌نظران انتخاب شدند. بنابراین تعداد و تنوع مصاحبه‌ها حجم نمونه آماری را تعیین می‌کند. فرایند مصاحبه به‌گونه‌ای اجرا شد که مصاحبه‌شوندگان درباره اجزای تشکیل‌دهنده امنیت شناختی سایبری نظرات خود را مطرح کنند و حتی این نظرات در مصاحبه‌های بعدی مورد پیگیری قرار گرفت. مصاحبه‌ها تا جایی ادامه پیدا کرد که مشخص شود که یافته‌ها تکرار می‌گردد و مصاحبه‌های جدید شناخت بیشتری نسبت به موضوع موردمطالعه به دست نمی‌دهند.

3-3- ابزار جمع‌آوری داده‌ها

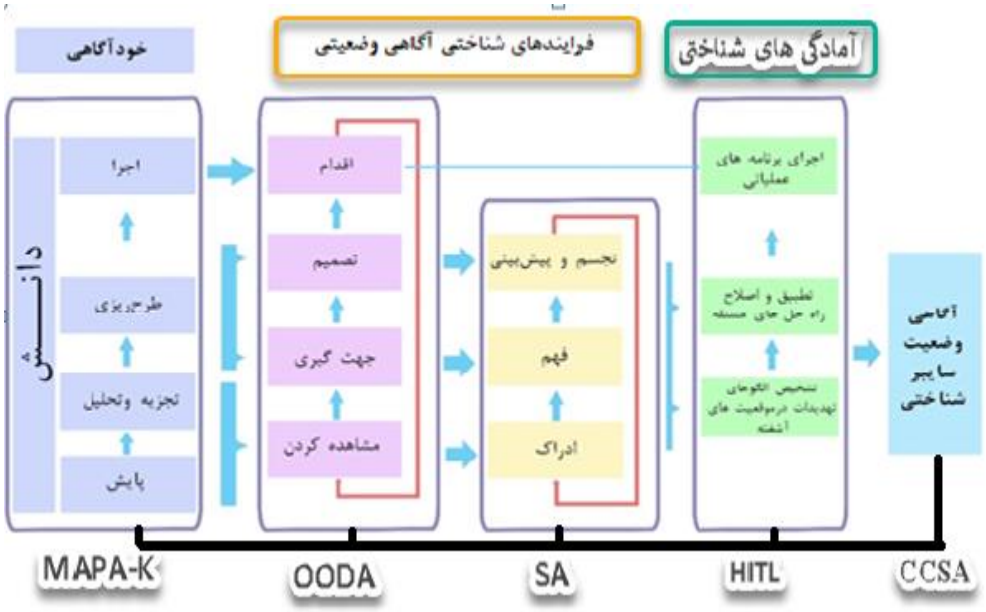
برای جمع‌آوری داده‌ها از ابزارهای مصاحبه و پرسشنامه استفاده شد. پس از اجرای روش فراترکیب و طی کردن مراحل هفت‌گانه، اجزاء و روابط مدل امنیت شناختی سایبری شناسایی شد و با استفاده از روش مصاحبه از متخصصان و خبرگان خواسته شد نظرات خود را درباره اجزاء و روابط مدل امنیت شناختی سایبری مطرح کنند، بدون اینکه مدل اولیه به آن‌ها عرضه شود. بر اساس نظرات خبرگان مدل اولیه را تکمیل و اصلاح گردید. نهایتاً برای اعتباریابی، مدل نهایی در اختیار متخصصان و خبرگان قرار گرفت و از آن‌ها خواسته شد تا نظرات خود را درباره آن ارائه دهند و از نتایج آن برای اصلاح و تعدیل نتیجه تحقیق استفاده شد.

4- یافته‌های پژوهش

4-1 - مدل امنیت شناختی

مدل پیشنهادی شناختی امنیت در شکل 4 نشان داده‌شده است که از اجزای آگاهی از وضعیت، خودآگاهی، اوودا و انسان در حلقه تشکیل گردیده است. مدل پیشنهادی سعی دارد تا از روند تلفیق داده‌ها، تولید دانش، مدل‌سازی نقشه‌های ذهنی و استفاده از داده‌های حجیم مرتبط با رویدادهای امنیتی سایبری پشتیبانی کند. هدف نهایی مدل پیشنهادی، ایجاد سطح بالایی از آگاهی وضعیتی سایبری با تقلید از فرایندهای شناختی انسانی با

تأکید بر نقش و جایگاه تحلیل‌گر امنیتی با تکیه بر آمادگی‌های شناختی و منابع مختلف اطلاعاتی برای تولید دانش است تا بهترین و مؤثرترین راهبردهای امنیتی سایبری را تعیین کند. چرخه اوودا دانش را از طریق سیستم‌های پیشنهاددهنده یا سیستم‌های پشتیبانی تصمیم، با تحلیلگر امنیت به اشتراک می‌گذارد. شکل 4 روابط بین هر یک از لایه‌های فناوری و هر یک از فرآیندهای شناختی تحلیلگر امنیتی را نشان می‌دهد. رصد مداوم وضعیت امنیت سایبری مبتنی بر کاربرد فرایند خودآگاهی است.



شکل 4. مدل مفهومی امنیت شناختی

مدل شناختی امنیت سایبری، گنجاندن الگوی انسان در حلقه را برای حل تعامل انسان با راه‌حل‌های فناوری لایه‌های مختلف انتخاب می‌کند، این رویکرد امکان ایجاد مدل‌های فهم ماشین[1] برای آموزش و خودکارسازی در راه‌حل‌های هوش مصنوعی و محاسبات خودمختار[2] را فراهم می‌آورد. در ضمن باعث تولید دانش و افزایش توانایی‌های شناختی تحلیلگر امنیت می‌گردد. الگوی انسان در حلقه تولید هشدارهای کاذب را کنترل می‌کند. این مدل همچنین کنترل محرک‌هایی که وظیفه اجرای پاسخ خودکار حادثه را دارند، بر عهده دارد تا از اقداماتی که می‌توانند روی سیستم‌های رایانه‌ای تأثیر منفی داشته باشند، بخصوص هنگام تولید هشدارهای کاذب، جلوگیری کند.

5- بحث و نتیجه‌گیری

[1] Machine understanding
[2] Autonomic computing

استفاده از علوم شناختی درزمینه امنیت سایبر به ما امکان می‌دهد تا در جهت بهبود فرآیندهای شناختی تحلیلگران امنیتی، به سهم روانشناسی، هوش مصنوعی، زبان‌شناسی و تعامل رایانه با انسان بپردازیم تا زمان پاسخ و اثربخشی تصمیم‌گیری در مورد اقدامات تشخیص، مهار یا کاهش یک حمله امنیتی بهبود یابد. امنیت شناختی به‌منظور تهیه نقشه‌های ذهنی، تلفیق داده‌های پیچیده، استفاده از داده‌های حجیم و نگهداری از دانش چهار مؤلفه: فرایندها، دانش، فناوری و توانایی‌های شناختی را در نظر می‌گیرد. برای مدیریت عملیات امنیتی درSOC ، باید بر پنج فرآیند کلان، ایجاد آگاهی وضعیت، مدیریت آسیب‌پذیری‌ها، مدیریت حوادث امنیتی، مدیریت وقایع امنیتی، فرایند کسب، یادگیری و انتقال دانش و مهارت تحلیلگران امنیتی تمرکز کرد. تولید یک شناخت در آگاهی از وضعیت را می‌توان با استفاده از سه فرآیند شناختی درک، فهم و پیش‌بینی (تجسم) به دست آورد. برای این فرآیند، داده‌های مربوطه را شناسایی، سپس داده‌ها تفسیر شده و در ارتباط قرار می‌گیرند و در انتها رویدادهای آینده ارزیابی و پیش‌بینی می‌شوند. باید در نظر بگیریم که همه کارها یا فرایندها به‌طور خودکار انجام نمی‌شود زیرا تأثیر اجرای یک عمل اشتباه ممکن است بیشتر از حمله امنیتی تأثیر منفی داشته باشد. برای رفع این معضل، نگه‌داشتن انسان در چرخه تصمیم‌گیری برای اجرای اقدامات یا وظایف مربوط به امنیت سایبر ضروری است. برای ایجاد رصد مستمر اطلاعات از منابع مختلف که امکان تولید شناخت و فرایند تصمیم‌گیری را فراهم می‌آورد، استفاده از تکنیک‌های کنترل و ارزیابی ضروری است. در زمینه علوم رایانه و امنیت سایبری برخی از مدل‌ها مانندMAPE-K ، OODA وHITL استفاده‌شده است. مدل امنیت شناختی پیشنهادی، راه‌حل‌های فناوری را با فرآیند شناختی و تکنیک‌های کنترل ادغام می‌کند که باعث ایجاد دید کاملی از آگاهی وضعیتی فضای سایبر می‌شود.

سرانجام، باید درک کرد که امنیت شناختی فقط به‌عنوان یک ابزار خودکارسازی برای جلوگیری از تهدیدهای سایبری نیست، بلکه این گزینه برای گسترش قابلیت‌های شناختی انسان (تحلیلگران و کارشناسان امنیتی) است تا بتواند با پردازش و تجزیه‌وتحلیل حجم زیادی از اطلاعات که از داده‌های ساختاریافته یا غیر ساختاریافته به دست می‌آید، بر اساس دانش حاصل‌شده، سرعت، دقت و اطمینان تصمیم‌گیری را افزایش دهد.

6. منابع:

یک). جی فردنبرگ، گوردون سیلورمن؛ مترجمان محسن افتاده‌حال و دیگران 1391. علوم شناختی؛ مقدمه‌ای بر مطالعه‌ی ذهن.

1. Al Sabbagh, B. & Kowalski, (2017), Socio-Technical SIEM (ST-SIEM): Towards Bridging the Gap in Security Incident Response. International Journal of Systems and Society (IJSS)

2. Amoud, M. and Roudies, 2016, O. MAPE-K-based approach for security @ runtime, doi:10.1109/SWSTE.2016.28.
3. Andrade. Roberto & Torres. Jenny(2018). Self-Awareness as an enabler of Cognitive Security
4. Andrade.R.O and S.G.Yoo/(2019)،Cognitivesecurity: A comprehensive study of cognitive science in cybersecurity
5. Baker. S, 1987, "The identification of the self, Psychological Review, no. 3, pp. 272–284,
6. Breton R, Rousseau R, 2018, THE C-OODA: a Cognitive Version of the OODA loop to represent C2 activities.
7. Camara J. and Kounev S. and Kephart J. and Milenkoski A. and Zhu X. Selfaware computing systems: related concepts and research areas, 2017, doi:10. 1007/978.3.319.47474.8.2
8. Cisco.(2018)Cognitivesecurity.[Online].Available:https://www.cisco.com/c/ en/us/about /corporate-strategy
9. ENISA, 2020,HOW TO SETUP UP CSIRT AND SOC دسامبر, ISBN 978-92-9204-410-7 - DOI 10.2824/056764
10. Etter, D.M. Foster, R.E. and Steele, T.P. (2000). Cognitive readiness and advanced distributed learning
11. Fletcher J. D. John E. Morrison, 2015, Cognitive Readiness
12. Ford. V. and Siraj. A, 2014, "Applications of machine learning in cyber security, in Conference: Conference: 27th International Conference on Computer Applications in Industry and Engineering
13. IBM. (2017) Security white paper. [Online]. Available: https://cognitivesecuritywhitepape r.mybluemix
14. IBM(2017): Applied cognitive security complementing the security analyst. https:// www.rsaconference.com.
15. Kaviani H, Hatami N, Shafieabadi, 2009, The impact of mindfulness-based cognitive therapy on the quality of life in non-clinically depressed people
16. Lafond. Daniel &Michel B. DuCharme,2012, Support Requirements for Cognitive Readiness in Complex Operations،Article in Journal of Cognitive Engineering and Decision Making DOI: 10.1177/1555343412446193
17. Lewis, P.R. and Chandra, A. and Parsons,2016, Self-awareness and self-expression: inspiration from psychology. In: Self-awareness computing systems. Natural computing series. Springer
18. McNeese, M.D. & Hall, D.L. (2017). The Cognitive Sciences of Cyber-Security: A Framework for Advancing Socio-Cyber Systems. Theory and Models for Cyber Situation Awareness.
19. Maymir.Fred -Ducharme, Lee. A. Angelelli,Douglas W Stapleton, 2015, Cognitive and Autonomic Cyber Defense
20. Marbán O. Segovia, J. Menasalvas, E. & Fernandez-Baizan, C. (2008). Towards Data Mining Engineering

21. Melore. M. (2018) The future of cognitive security is now. [Online]. Available: https://securityintelligence.com/ the-future-of-cognitive-security-is-now/
22. Miller, 2003, The cognitive revolution: a historical perspective.
23. Murray. S(2016)Human skills are essential in battle against cyber crime.https://www.ft.com/content/46449768-7031-11e6-a0c91365ce54b926
24. NIST.(2016)Cognitivesecurity.[Online].Available:https://www.nist.gov/sites/default/files/ documents /2016/09/16
25. Pino R, Kott A, Shevenell M. 2014, Cybersecur Syst Hum Cognit Augment. doi:10.1007/978-3-31910374-7.
26. Rouse.M.(2017),Cognitivesecurity.[Online].Available:https://whatis.techtarget.com/definition/cognitive-security
27. Scott J, Rebekah.B,2017, Intelligence driven incident response. O Reilly books.
28. Timonen. J, 2015, Improving situational awareness of cyber physical systems based on operator's goals. In:international conference on cyber situational awareness, data analytics and assessment (CyberSA)
29. Thomas W, Manz D, 2017, Research methods for cybersecurity. Elsevier
30. Torres. Jenny, 2018,Self-Awareness as an enabler of Cognitive Security
31. Varela FJ, Thompson E, Rosch E. 2017, The embodied mind: Cognitive science and human experience: MIT press