بیست و دومین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات
The 22th National Conference on Computer Science and Engineering and Information Technology
April 2024 – فروردین ۱۴۰۳

ارزیابی سطح بلوغ امنیت در شرکت های ارائه دهنده خدمات پرداخت (PSP)

امیر روحانی[۱] ، محمد سعید محمدزاده چالکی [۲]

[۱] کارشناسی ارشد مدیریت فناوری اطلاعات، مدیریت سیستم‌های اطلاعاتی، دانشگاه آزاد واحد بناب

[۲] کارشناسی ارشد مدیریت فناوری اطلاعات، کسب‌وکار الکترونیک، دانشگاه علم و صنعت ایران

چکیده

در دنیای امروز، امنیت سایبری به دغدغه‌ای مهم برای سازمان‌ها در هر اندازه و صنعتی تبدیل شده است. هکرها و مجرمان سایبری دائماً در حال تکامل روش‌های خود هستند و سازمان‌ها باید برای مقابله با آن‌ها، اقدامات پیشگیرانه‌ای را اتخاذ نمایند. یکی از گام‌های مهم در این مسیر، ارزیابی سطح بلوغ امنیت سازمان است. با توجه به نقش حیاتی شرکت‌های ارائه دهنده خدمات پرداخت (PSP) در تراکنش های مالی، تضمین امنیت اطلاعات و سیستم ها از اهمیت بالایی برخوردار است. ارزیابی سطح بلوغ امنیت، ابزاری کارآمد برای سنجش وضعیت فعلی امنیت سایبری در PSP ها و شناسایی نقاط ضعف و قوت آن ها به منظور ارتقای سطح امنیت ارائه می‌دهد. بنابراین، این پژوهش با هدف توسعه متدلوژی برای شناسایی سطح بلوغ امنیت سایبری در شرکت‌های ارائه دهنده خدمات پرداخت (PSP) است. این روش بر اساس دو مرحله است. گام اول مربوط به شناسایی دارایی ها، تهدیدها و تأثیرات آن‌هاست و مرحله دوم مربوط به تجزیه و تحلیل و طبقه بندی الزاماتی است که در گروه هایی طبقه بندی شده اند. این تجزیه و تحلیل اجازه می دهد تا سطح بلوغ یک مورد خاص را مشخص سازیم.

واژگان کلیدی: ارزیابی سطح بلوغ امنیت، مدل بلوغ امنیت سایبری، ارائه دهنده خدمات پرداخت، PSP

The 22th National Conference
18/04/2024-(Mazandaran)
Elmavaran Danesh Group
R.S. Institute
Article Code: NCCIT -117006

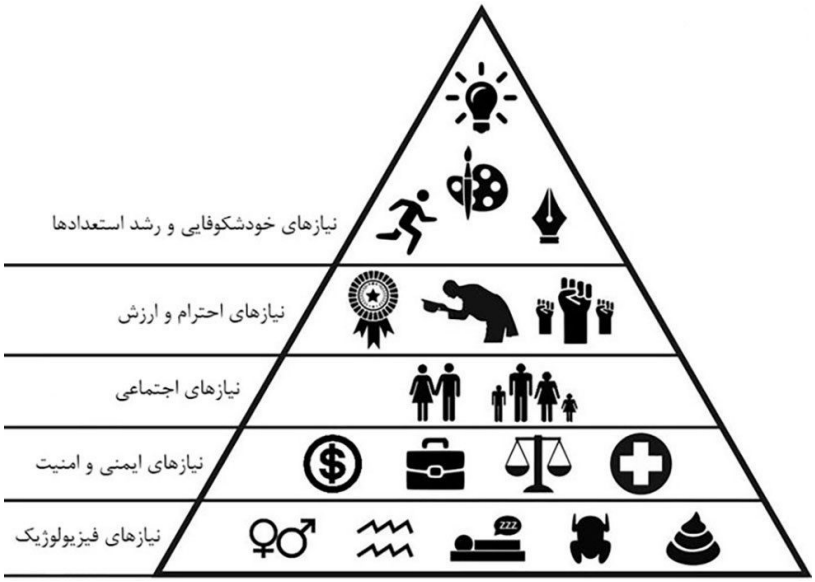
Indexing Accepted Articles in Civilica

مقدمه

امروزه توانایی نفوذ در فضای سایبر به عنوان یکی از مهمترین منابع قدرت در قرن ۲۱ محسوب می‌شود، لذا بازیگران دولتی و غیردولتی برای دست یافتن به اهداف نظامی،ایدئولوژیک و اجتماعی در فضای سایبر یا فضای فیزیکی از این قدرت بهره می‌گیرند. زیرساخت‌های حیاتی از دارایی‌های مهم امنیت عمومی، رفاه اقتصادی و امنیت ملی کشورها محسوب می‌شوند. مرور وقایع و حوادث سایبری در سال‌های اخیر کشور، مؤید این واقعیت است که بخش قابل توجه تهدیدات علیه کشور، علی‌الخصوص در زیرساخت‌های حیاتی، مستقیما از فضای سایبری نشات می‌گیرند و یا این فضا را مورد هدف قرار می‌دهند. فضای سایبری هیچگونه حد و مرزی ندارد و با کمترین هزینه و از هر نقطه جهان میتوان مورد هجوم قرار گیرد، امروزه تهدیدات سایبری یکی از بزرگترین چالش‌های پیش روی حوزه امنیت زیرساخت‌ها، علی‌الخصوص شرکت‌های ارائه دهنده خدمات پرداخت(PSP)، محسوب می‌گردد. به همین جهت، ایجاد سیاست‌های ایمن‌سازی امنیت سایبری برای زیرساخت‌های حیاتی، در دستور کار اکثر کشورها و همچنین سازمان پدافند غیرعامل کشور ایران قرار گرفته است. بدین منظور این پژوهش به دنبال ارائه مدل مفهومی و متدولوژی شناسایی بلوغ امنیت سایبری برای شرکت های ارائه دهنده خدمات پرداخت به عنوان یکی از زیرساخت‌های حیاتی کشور با تمرکز بر استانداردهای مدیریت امنیت سایبری و واکاوی مدل‌های بلوغ امنیت سایبری با مشخص ساختن مؤلفه‌های مدل بلوغ امنیت سایبری است. مدل به دست آمده می‌تواند منتج به افزایش ایمن‌سازی شرکت‌های ارائه دهنده خدمات پرداخت(PSP) در حوزه سایبری و تصمیم‌گیری مدیران آن شرکت‌ها برای پیاده‌سازی مدل بلوغ امنیت سایبری و ارزیابی وضعیت امنیت سایبری در شرکت‌های ارائه دهنده خدمات پرداخت گردد.

بیان مسئله

انسان دارای سلسله نیازهای مختلف است که اساسی ترین آن‌ها گستره فیزیولوژیکی همانند تنفس و غذا خوردن را در بر می‌گیرد. پس از تأمین این نیازها در مرحله بعدی، نیازهای امنیتی شامل ثبات، وابستگی، حفاظت، رهایی از ترس و اضطراب، قانون و نظم است. مازلو نیز نیازهای حیاتی انسان را در یک هرم طبقه‌بندی و توصیف می‌کند به طوری که مازلو انسان را به عنوان موجودی در جستجوی امنیت تعریف می‌کند و بر این باور است که موجودات زنده تحت سلطه این نیازها به دنبال اکتساب گزاره‌های امنیتی می‌باشند. (شکل ۱) (Poston, 2009) .



شکل (۱) هرم نیاز های مازلو (Poston,2009)

اگرچه ایمنی و امنیت در هرم مازلو در درجه دوم نیازهای فیزیولوژیکی هستند، اما این دو از یکدیگر جدایی ناپذیرند؛ به عنوان مثال، نیاز به امنیت منابع غذایی و آب نشان می‌دهد که چگونه امنیت می‌تواند بر نیازهای فیزیولوژیکی تأثیر بگذارد. تأمین این امنیت گستره‌ای از انبارهای کوچک تأمین غذا در روستاها تا زیرساخت‌های حیاتی کشور همانند شبکه توزیع برق، شبکه توزیع سوخت، شبکه حمل و نقل، ارتباطات و دیگر زیرساخت‌ها را نیز در بر میگیرد. (دانایی فرد، ۱۳۸۹).

برای جلوگیری از جرایم سایبری، لازم است با استفاده از اقدامات امنیتی سایبری گسترده و به روز از زیرساخت‌های حیاتی کشور برای به حداقل رساندن خطرات حملات سایبری محافظت نماییم. امنیت سایبری و امنیت اطلاعات دارای نقاط مشترک بسیاری هستند اما این دو از یکدیگر متمایزند. بر طبق استاندارد ISO 27032 امنیت اطلاعات به حفاظت از داده‌ها و امنیت سایبری بر پیشگیری و یا توقف حملات سایبری از طریق افزایش امنیت برنامه‌ها، امنیت شبکه و امنیت اینترنت تمرکز می‌کند. لازم به ذکر است درک رابطه بین این حوزه‌های امنیتی، جهت تأمین امنیت زیرساخت شرکت‌های ارائه دهنده خدمات پرداخت امری ضروری است که در شکل (۲) چگونگی این روابط مشخص گردیده است (ISO/IEC 27032:2023).

شکل (۲) رابطه بین امنیت سایبری و حوزه های مرتبط (ISO/IEC27032:2023)

از آنجا که افزایش سطح رفاه عمومی، توسعه اقتصادی، ارتقای توان دفاعی و امنیتی کشور در گرو تأمین امنیت زیرساخت‌های حیاتی کشور در حوزه‌های انرژی، فناوری اطلاعات و ارتباطات، حمل و نقل، بانکداری و دیگر حوزه‌ها است، پژوهش حاضر ارائه مدل مفهومی بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور را در دستور کار خود قرار داده است، که این مهم با واکاوی مدل‌های بلوغ امنیت سایبری و شناخت فضای امنیت سایبری زیرساخت‌ها فراهم خواهد آمد.

برای ارائه روشی مناسب جهت افزایش سطح بلوغ امنیت در هر سازمانی، ابتدا می‌بایست با یک روش مناسب و هدفمند به ارزیابی سطح بلوغ امنیت در سازمان پرداخت. ارزیابی سطح بلوغ امنیت، فرآیندی برای سنجش وضعیت فعلی امنیت سایبری سازمان در مقایسه با بهترین روش‌ها و استانداردهای صنعت است. این ارزیابی به سازمان‌ها کمک می‌کند تا نقاط قوت و ضعف خود را در زمینه امنیت سایبری شناسایی کرده و برنامه‌ای برای ارتقای سطح امنیت خود تدوین کنند.

ضرورت و اهمیت پژوهش

اهمیت

با ورود جهان به عصر اطلاعات دیجیتال، دولت‌ها و شرکت‌ها به فناوری اطلاعات وابستگی پیدا کرده‌اند که این وابستگی در راستای بهینه‌سازی عملکردها، هوشمند سازی فرایندهای کسب‌وکار و ارائه خدمات از راه دور، افزایش پیدا نموده است. همه‌گیری کرونا فرصتی برای توسعه بیشتر دولت الکترونیکی و خدمات الکترونیکی فراهم آورد و

دستگاه‌های مختلف نیز به خوبی از این فرصت استفاده کردند. بدین ترتیب فناوری اطلاعات و امنیت اطلاعات و سایبری نیز جایگاه ویژه‌ای در عرصه دیجیتال یافته است. (Nye, 2009) .

زیرساخت‌های حیاتی از مهمترین دارایی‌های امنیت عمومی هر کشور محسوب می‌شود و ثبات و پایداری این زیرساخت‌ها رفاه اقتصادی و امنیت ملی کشورها را رقم میزند. غالبا سیستم‌های سایبری برای نظارت و کنترل زیرساخت‌های حیاتی استفاده می‌گردند که تعدادی از زیرساخت‌ها از طریق بستر فناوری اطلاعات به اینترنت متصل می‌شوند. بنابراین امنیت سایبری یکی از موارد مهم در دستور کار امنیت ملی هر کشور است.

به لحاظ نظامی، قدرت سایبری، شاید مهم‌ترین قدرت نوظهور چند دهه گذشته باشد. در حال حاضر اغلب نیروهای مسلح کشورها برای ایمن‌سازی مرزهای سایبر و فرا سایبری خود در برابر چنین تحول جدیدی آماده می‌شوند. رهنامه‌های جدید نظامی بر اساس فضای سایبر تدوین می‌شوند. در تمام سطوح منازعه، از شورش‌های داخلی گرفته تا جنگ متعارف، قدرت سایبری، عامل حتمی و گریزناپذیر توانمندی نظامی است (آذر،۱۴۰۱).

در این پژوهش هدف دوم از پنج هدف اصلی پدافند غیرعامل در سیاست‌های ابلاغی از سوی نهاد مربوطه یعنی تداوم فعالیت ضروری مورد بررسی قرار گرفته است. بنابراین، نظر به اینکه فضای سایبری هیچگونه حد و مرزی ندارد و با کمترین هزینه و از هر نقطه جهان میتوان هدف را مورد حمله قرارداد، تهدیدات سایبری را میتوان یکی از بزرگترین چالش‌های پیشروی حوزه امنیت زیرساخت‌های حیاتی قلمداد کرد (اختری، ۱۴۰۱).

برای بیان ضرورت انجام فرایند ارزیابی سطح بلوغ امنیت ابتدا به بیان بخشی از مزایای انجام این امر پرداخته می‌شود.

- شناسایی نقاط ضعف و قوت: این ارزیابی به سازمان کمک می‌کند تا بخش‌هایی از سیستم‌های خود را که در معرض خطر هستند، شناسایی کرده و برای رفع آن‌ها اقدام نماید.
- بهبود وضعیت امنیت: با شناسایی نقاط ضعف، می‌توان برنامه‌ای برای ارتقای سطح امنیت سازمان تدوین و اجرا کرد.
- کاهش ریسک: با ارتقای سطح امنیت، ریسک وقوع حملات سایبری و ضررهای مالی و جانی ناشی از آن کاهش می‌یابد.
- افزایش اعتماد مشتریان: مشتریان و شرکای تجاری سازمان زمانی که بدانند یک سازمان به امنیت سایبری خود اهمیت می‌دهد، بیشتر به مجموعه اعتماد می‌کنند.

ضرورت

در دنیای امروز، امنیت سایبری به یکی از مهم‌ترین دغدغه‌ها برای سازمان‌ها تبدیل شده است. حملات سایبری روز به روز پیچیده‌تر و مخرب‌تر می‌شوند و سازمان‌ها را در معرض خطر از دست رفتن اطلاعات، اختلال در سرویس‌دهی و ضررهای مالی قرار می‌دهند. پیدایش و گسترش سریع فضای سایبر و اتکا روزافزون کشورها به قابلیت‌های بی‌شمار آن، روزبه‌روز به تهدیدها، آسیب‌پذیری‌ها و جرایم این فضا افزوده و جنگ بین کشورها از فضای واقعی به فضای سایبری کشیده شده است، همچنین شکل جنگ‌ها در کنار جنگ‌های سخت به جنگ سایبری با عنوان بعد پنجم جنگ‌ها تغییر یافته است (سپهری، ۱۴۰۰).

ازاین‌رو و با توجه به اینکه در سال‌های اخیر حجم حملات سایبری به زیرساخت‌های حیاتی کشور، توسط دولت‌های متخاصم افزایش یافته است، ارائه یک مدل بلوغ امنیت سایبری برای زیرساخت‌های شرکت‌های ارائه دهنده خدمات پرداخت (PSP) ، جهت بالا بردن ضریب تاب‌آوری و امنیت سایبری زیرساخت‌های حیاتی مورد نیاز است و انجام چنین تحقیقاتی موارد ذیل را به دنبال خواهد داشت.

- ایجاد مواضع فعالانه در برابر حملات سایبری.
- افزایش قدرت دفاع سایبری در حوزه زیرساخت امنیت سایبری.

انجام ارزیابی سطح بلوغ امنیت (SMA) به سازمان‌ها کمک می‌کند تا وضعیت فعلی امنیت سایبری خود را در مقایسه با سطوح ایده‌آل و بهینه‌ی آن سنجش کنند. این ارزیابی به آن‌ها در شناسایی نقاط قوت و ضعف خود در زمینه امنیت سایبری و تدوین برنامه‌ای برای ارتقای سطح امنیت خود کمک می‌نماید.

چه زمانی باید ارزیابی سطح بلوغ امنیت یا SMA انجام شود؟

- **هنگام تاسیس یک سازمان جدید**: SMA به سازمان‌های جدید کمک می‌کند تا از همان ابتدا سطح امنیت خود را بر اساس به‌روش‌ها[1] بنا کنند.
- **پس از بروز یک حمله سایبری:** انجام ارزیابی سطح بلوغ امنیت به سازمان‌ها کمک می‌کند تا نقاط ضعف امنیتی خود را که منجر به بروز حمله شده است، شناسایی و رفع کنند.
- **به طور دوره‌ای:** SMA باید به طور دوره‌ای انجام شود تا از به‌روز بودن سطح امنیت سازمان اطمینان حاصل شود.

چه کسانی باید در SMA مشارکت کنند؟

[1] Best Practices

مدیریت ارشد: مدیریت ارشد باید متعهد به ارتقای سطح امنیت سایبری سازمان باشد و از SMA به عنوان ابزاری برای دستیابی به این هدف استفاده نماید.

کارکنان IT : کارکنان IT مسئول پیاده‌سازی و مدیریت الزامات و کنترل های ارزیابی سطح بلوغ امنیت هستند و باید در SMA مشارکت فعال داشته باشند.

کارکنان سایر بخش‌ها: کلیه کارکنان در حفظ امنیت سایبری سازمان نقش دارند و باید در انجام فرایند SMA مشارکت فعال داشته باشند.

اهداف پژوهش

هدف این پژوهش، ارائه مدل مفهومی بلوغ امنیت سایبری برای شرکت‌های ارائه دهنده خدمات پرداخت (PSP) به عنوان یکی از مهم‌ترین زیرساخت های حیاتی کشور با رویکرد فراترکیب است. بر این اساس در مرحله نخست با مطالعه نظام‌مند ادبیات موضوع بلوغ امنیت سایبری و با استفاده از روش فراترکیب، همچنین مطالعه و بررسی مدل‌های مختلف بلوغ امنیت سایبری، استانداردهای ایمن‌سازی زیرساخت‌های حیاتی، استانداردهای امنیت اطلاعات و امنیت سایبری، مدلی برای ایمن‌سازی زیرساخت‌های حیاتی با استفاده از مدل‌های بلوغ امنیت سایبری پیشنهاد می‌گردد.

هدف اصلی پژوهش:

- طراحی مدل مفهومی بلوغ امنیت سایبری برای شرکت‌های ارائه دهنده خدمات پرداخت (PSP)
- ارائه روش‌های جدید جهت ارزیابی سطح بلوغ امنیت در شرکت‌های ارائه دهنده خدمات پرداخت (PSP)

اهداف فرعی پژوهش:

- شناسایی ابعاد، مؤلفه‌ها و شاخص‌های مدل بلوغ امنیت سایبری برای شرکت‌های ارائه دهنده خدمات پرداخت (PSP)
- مشخص شدن روش طراحی مدل مفهومی بلوغ امنیت سایبری برای شرکت‌های ارائه دهنده خدمات پرداخت (PSP)

مبانی نظری و پیشینه‌های پژوهش

مبانی نظری

- مدل ISO/IEC 27001: این مدل یک استاندارد بین‌المللی برای مدیریت امنیت اطلاعات است و شامل الزاماتی برای مدیریت ریسک، کنترل دسترسی، رمزنگاری و سایر اقدامات امنیتی است.
- مدل CMMI for Security: این مدل بر اساس مدل CMMI (Capability Maturity Model Integration) برای توسعه نرم‌افزار است و به سازمان‌ها کمک می‌کند تا فرآیندهای امنیتی خود را بهبود بخشند.
- فضای سایبری: فضایی فیزیکی و عینی شامل تجهیزات سخت‌افزاری و ملزومات فناوری اطلاعات و ارتباطات است که این فضا دربرگیرنده ابعاد غیر فیزیکی ازجمله اطلاعات، نرم‌افزارها، پردازش و خدمات مرتبط با اطلاعات است که جهت همبستگی متقابل بین عوامل انسانی از طریق فضای مجازی متکی به شبکه‌های اینترنتی و تجهیزات مخابراتی به وجود می‌آید (ولوی، ۱۴۰۰).
- زیرساخت‌های حیاتی: زیرساخت به مجموعه عناصر ساختاری به هم پیوسته‌ای اطلاق می‌شود که یک سیستم بزرگ را تشکیل داده و دارای ابعاد فنی و فناورانه گسترده‌ای است و در صورت عملکرد صحیح همه بخش‌های آن، می‌توان عرضه خدمات را به نحوه مطلوبی انتظار داشت. در یک تقسیم‌بندی کلی، میتوان زیرساخت‌ها را به دو نوع حیاتی و غیر حیاتی طبقه‌بندی کرد. با این تقسیم‌بندی قائل به این هستیم که اهمیت برخی از زیرساخت‌ها نسبت به برخی دیگر بیشتر است. با توجه به این تفکیک به نظر می‌رسد زیرساخت‌های حیاتی را میتوان به زیرساخت‌های مرتبط با امنیت ملی یک کشور مرتبط دانست (کاوند، ۱۳۹۹).
- زیرساخت‌های حیاتی اصطلاحی است که برای توصیف دارایی‌هایی استفاده می‌شود که برای عملکرد و امنیت یک جامعه اقتصادی در هر کشور ضروری است (ITU,2008).
- مدل بلوغ: مفهوم مدل‌های بلوغ به‌طور فزاینده‌ای در حوزه سیستم‌های اطلاعاتی به عنوان یک رویکرد برای توسعه سازمانی یا به عنوان وسیله‌ای برای ارزیابی سازمانی استفاده شده است. هر چارچوب نظام‌مندی برای انجام الگوبرداری و بهبود عملکرد میتواند یک مدل باشد و در صورتی که دارای فرآیندهای بهبود مستمر باشد میتواند یک مدل بلوغ به حساب آید (اخوان، ۱۳۹۹).
- مدل بلوغ امنیت سایبری: مدل‌های بلوغ امنیت سایبری با درک طیف گسترده‌ای از امنیت تا ناامنی تعیین می‌شود، این مدل‌ها به عنوان یک ابزار سنجش برای اندازه‌گیری تفاوت بین وضعیت سطح امنیت فعلی و سطحی که می‌خواهیم به آن برسیم به کار گرفته می‌شود. افزون بر آن و با توجه به وابستگی زیرساخت‌های حیاتی به بستر فناوری و فضای سایبر، تدوین دستورالعمل و ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌ها امری ضروری است که این موضوع مستلزم شناخت دقیق شاخص‌های موجود در مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات است.
- مدل NIST Cybersecurity Framework: این مدل توسط موسسه ملی استانداردها و فناوری آمریکا (NIST) ارائه شده است و شامل پنج بخش اصلی است: شناسایی، محافظت، تشخیص، پاسخ و بازیابی.

پیشینه‌های پژوهش

پیشینه مطالعات داخلی

- اخوان و رادفر، در پژوهشی با عنوان «ارائه مدلی برای پایش بلوغ امنیت اطلاعات»، مدل‌های بلوغ امنیت اطلاعات مورد بررسی قرارداده و با توجه به نظر خبرگان و یافته‌های پژوهش مدلی متشکل از ۵ مرحله برای پایش امنیت اطلاعات ارائه کرده‌اند (شکل ۳)، شمای کلی مدل بلوغ امنیت اطلاعات ارائه شده توسط ایشان را نمایش می‌دهد (اخوان و رادفر، ۱۳۹۹). این پژوهش در یکی از شرکت‌های زیرمجموعه صنعت نفت انجام شده است و پایه آن بر اساس الزامات استاندارد ISO 27001 است.
- در پژوهشی دیگر با عنوان «بررسی انواع راهکارهای افزایش امنیت در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی»، دفاع در عمق را یکی از مهمترین و پرکاربردترین راهبرد در ایمن‌سازی سیستم‌های کنترل صنعتی برشمرده است و رابطه امنیت سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی با توجه به ماهیت اجزای تشکیل دهنده این سیستم‌ها به صورت شکل (۳) ترسیم شده است.

شکل (۳) رابطه امنیت سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی (افشار و همکاران، ۱۳۹۷)

- همچنین در این پژوهش به بحث و توضیح این راهکارها در قالب دو دسته پایه‌ای و ساختاری پرداخته شده است (افشار و همکاران، ۱۳۹۷).
- میریوسفی و غفاری، در پژوهشی نسبت به بررسی «راهبردهای نوین حفاظت از زیرساختهای حیاتی» پرداخته است. در این پژوهش برخی شیوه‌ها و راهبردهای ملی برای حفاظت از زیرساخت‌های حیاتی بیان شده و چالش‌ها و الزامات پیش روی حفاظت از زیرساخت‌ها تبیین شده است (میریوسفی، ۱۳۹۹)

- در پژوهشی دیگر، به روش مطالعه تطبیقی نسبت به تعیین شاخص‌های ارزیابی امنیت سایبری پرداخته شده است. در این پژوهش با استناد به منابع کتابخانه‌ای و بررسی گزارش‌های ارائه شده از سوی مراجع معتبر در حوزه امنیت سایبری، هفت الگوی ارزیابی معتبر انتخاب و با رویکرد تطبیقی نسبت به بررسی ابعاد، اهداف و رویکرد آنها اقدام شده است (سعادتمند و همکاران ۱۴۰۰).

پیشینه مطالعات خارجی

- در پژوهشی با عنوان «مدل پرسشنامه‌ای برای ارزیابی بلوغ امنیت سایبری در زیرساختهای حیاتی» با استفاده از پرسشنامه و بررسی انواع مدل‌های بلوغ امنیت سایبری، یک مدل برای ارزیابی و بهبود امنیت سایبری برای ارائه دهندگان خدمات و مدیران زیر ساخت‌های حیاتی ارائه شده است (Y.Bilge , 2019).
- بیلگ و دیگران در پژوهشی با عنوان «مدل بلوغ امنیت سایبری مبتنی بر آسیب‌پذیری برای اندازه‌گیری آمادگی حفاظت از زیرساخت‌های حیاتی ملی» یک مدل بلوغ امنیت سایبری مبتنی بر آسیب‌پذیری برای اندازه‌گیری زیرساخت‌های حیاتی در کشور ترکیه را با استفاده از نظرات خبرگان و واکاوی مدل‌های مشهور بلوغ امنیت سایبری ارائه کرده است (K.Blige, 2019).
- در پژوهشی که در قالب یک رساله دکتری با عنوان «مدل بلوغ قابلیت امنیت سایبری برای زیرساخت‌های فناوری اطلاعات حیاتی در سازمان‌های مالی نیجریه» انجام شده است، مدل بلوغ قابلیت امنیت سایبری (C2M2) برای سازمان‌های مالی نیجریه به عنوان یک مدل امنیتی برای تعیین سطح قدرت امنیت سایبری در سازمان‌های مالی نیجریه برگزیده شده است. این مدل توسعه‌ای پنج سطح بلوغ را ارائه کرده است (جدول ۱).

سطوح شاخص بلوغ - Maturity Indicator Levels [MILs]	هفت دامنه مدل: گروه بندی منطقی اقدامات امنیت سایبری ۷ Model Domain: Logical Grouping of Cybersecurity Practices							هر سلول حاوی تعریف است (Each Cell Contain the Defining)
	مقررات قانونی (Legal Regulation)	حکمرانی (Governance)	کنترل دسترسی (Access Control)	مدیریت ریسک (Risk) (Management	فرهنگ امنیت (Security Culture)	مدیریت تکنولوژی (Technology) (Management	مدیریت رخدادها Incident) (Management	
۴-خلاقانه (Innovation)								
۳- پیشرفته (Advanced)								
۲- تکامل یافته (Progressed)								
۱- پایه‌ای (Basic)								
۰- هیچ چیز وجود ندارد (Nothing Exist)								
MiLs:۵ تعریف پیشرفت عملکردها - Define Progressions of Practices								

جدول (۱) مدل بلوغ قابلیت امنیت سایبری برای زیرساخت‌های حیاتی فناوری اطلاعات در سازمان‌های مالی نیجریه

- هدف این پژوهش ایجاد مدلی است که سطح قدرت امنیت سایبری در سازمان‌های مالی نیجریه را افزایش دهد (Idle, 2019:36).

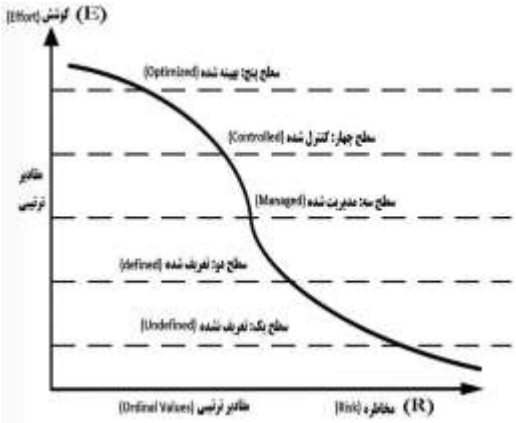
انواع مدل‌های بلوغ امنیت اطلاعات

مدل بلوغ امنیت اطلاعات – Information Security Maturity Model (ISMM) :

هدف از ارائه مدل بلوغ ISMM این است که شرکت‌ها و سازمان‌ها بتوانند وضعیت پیاده‌سازی اقدامات انجام شده در خصوص امنیت اطلاعات را اندازه‌گیری نمایند. این مدل در اوایل سال ۲۰۱۱ به عنوان فرآیندی برای مدیریت، اندازه‌گیری و کنترل شیوه‌های مدیریت امنیت اطلاعات انتشار یافت .اساس شکل‌گیری ISMM دقیقا مشخص نیست ولی ارائه‌دهنده این مدل با بهره‌گیری از چهارچوب COBIT[2] و ،TOGAF[3] چهار دامنه برای آن ترسیم کرده است که این دامنه‌ها عبارتاند از: حاکمیت شرکتی، معماری سیستم، مدیریت خدمات و فرهنگ سازمانی (Saleh, 2011).

مدل بلوغ امنیت اطلاعات (دولت الکترونیک) – (E-Government) Information Security Maturity Model (ISMM) :

مدل E-Government ISMM در اوایل سال ۲۰۱۱ برای اندازه‌گیری بلوغ حوزه‌های فنی و اجتماعی (غیر فنی) در شیوه‌های امنیت اطلاعات ایجاد شده است. این مدل برای شرکت‌هایی ایجاد شده است که خدمات دولتی ایمن ارائه می‌کنند. با استفاده از این مدل، شرکت‌ها می‌توانند میزان (بلوغ) اقدامات در حوزه امنیت اطلاعات خود را اندازه گیری کنند. برخلاف مدل‌های ISMM، که قبلا توسعه یافته است، این مدل هم کمیت و هم کیفیت خدمات دولتی را اندازه گیری می‌کند (Karakola, 2011).



نمودار (۱) مدل E-Government ISMM

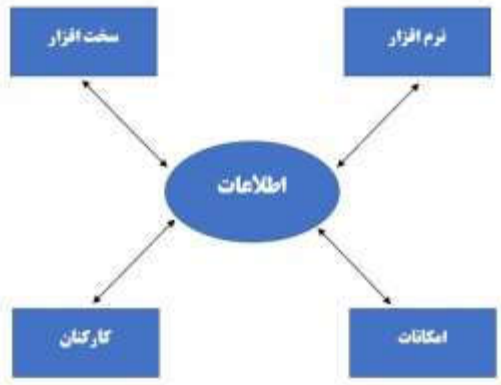
[2] Control Objectives for Information and Related Technologies
[3] The Open Group Architecture Framework

پنج مرحله امنیت اطلاعات – Five Stage to Information Security (5S2IS):

این مدل برای پیاده‌سازی مدیریت امنیت اطلاعات در شرکت‌های کوچک و متوسط [4]مورد استفاده قرار می‌گیرد. حتی شرکت‌هایی که قصد دریافت گواهینامه مرتبط با امنیت اطلاعات را ندارند می‌توانند از این مدل برای توسعه امنیت اطلاعات استفاده کرده و اقداماتی را جهت کاهش خطرات سایبری انجام دهند(Gillies, 2011). این مدل در اواسط سال ۲۰۱۱ بر اساس استانداردهای ISO27001, ISO27002 و مدل بلوغ قابلیت هامفری[5] استوار است (Humphrey, 1989).

سطوح بلوغ امنیت اطلاعات – GAIA Maturity Level Information Security (GAIA-MLIS) :

هدف مدل GAIA-MLIS افزایش آگاهی شرکت‌ها از سطح بلوغ آن‌ها در سیستم امنیت اطلاعات است. این امر با ارائه افزایش آگاهی از نقاط ضعف و قوت آن‌ها صورت می‌گیرد. این مدل بر اساس وضعیت شرکت، توصیه‌های مشخصی را در خصوص بهبود امنیت اطلاعات ارائه می‌دهد، هدف این مدل تعیین نقاط ضعف و کمک به بهبود و مدیریت در پنج حوزه، اطلاعات، سخت‌افزار، نرم‌افزار، امکانات، کارکنان است (شکل ۴).



شکل (۴) مدل GAIA-MLIS

مدل بلوغ ناحیه تمرکز امنیت اطلاعات – Information Security Focus Area Maturity Model (ISFAM) :

[4] SME (Small and medium-sized enterprises)
[5] Humphrey

مدل ISFAM در اوایل سال ۲۰۱۴ توسط اسپرویت و رولینگ [6]توسعه یافته است. این مدل بر حوزه امنیت اطلاعات متمرکز است، همچنین قادر به تعیین سطح فعلی بلوغ امنیت اطلاعات است و می‌تواند برای بهبود تدریجی و ساختاری بلوغ امنیت اطلاعات در سازمان مورد بهره‌برداری قرار گیرد (Spruit, 2014).

مدل مذکور برگرفته از استانداردهای ISO27002:2005، سرفصل‌های دوره، CISSP، استانداردهای منتشر شده در انجمن «بهترین روش‌ها برای امنیت اطلاعات[7]»، چارچوب امنیت اطلاعات (ISO-light) و چارچوب IBM است.

ناحیه تمرکز - (Focous Area)	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
سازمانی – (Organizational)													
۱- مدیریت ریسک (Risk Management)				A		B		C			D		
۲- توسعه سیاست (Policy Development)			A		B						C		
۳- سازماندهی امنیت اطلاعات (Organizing Information Security)		A			B					C		D	
۴- امنیت منابع انسانی (Human Resource Security)				A		B		C		D			
۵- انطباق (Compliance)				A		B						C	
فنی – (Technical)													
۶- مدیریت هویت و دسترسی (Identiti and Access Management)					A		B		C		D		
۷- توسعه نرم افزار به صورت امن (Secure software development)					A		B			C		D	
فنی و سازمانی – (Organizational and Technical)													
۸- مدیریت رخدادها (Incident Management)			A			B			C			D	
۹- مدیریت تداوم کسب و کار (Business Continuity management)				A		B		C			D		E
۱۰- مدیریت تغییرات (Incident Management)				A		B		C		D			
پشتیبانی – (Support)													
۱۱- امنیت فیزیکی و محیطی (Physical and Environment security)						A		B		C			D
۱۲- مدیریت دارایی (Assets management)			A				B			C		D	
۱۳- معماری (Architecture)				A		B			C		D		

جدول (۲) مدل ISFAM (Spruit,2014)

انواع مدل‌های بلوغ امنیت سایبری

مدل بلوغ امنیت سایبری جامع – Community Cyber Security Maturity Model (CCSMM) :

این مدل برای کمک به شرکت‌ها و جوامع مختلف برای ایجاد برنامه‌های امنیت سایبری و افزایش آگاهی در مورد خطرات سایبری توسعه یافته است. هدف این مدل ارائه ابزارهایی برای توسعه و بهبود امنیت سایبری برای استفاده کنندگان است. مدل بلوغ CCSMM یک معیار برای اندازه‌گیری وضعیت امنیت سایبری و سطح بلوغ ارائه می‌کند، در نهایت یک نقشه راه برای بهبود

[6] Spruit and Roling
[7] Good Practice of the Information Security

وضعیت امنیت سایبری و همچنین یک نقطه مرجع و اصطلاحاتی مشترک برای استفاده کنندگان به ارمغان می‌آورد (White,2007).

ابتکار ملی برای آموزش امنیت سایبری - مدل بلوغ قابلیت – National Initiative for Cybersecurity Education – Capability Maturity Model (NICE) :

مدل NICE برگرفته از مفهوم «ابتکار یکپارچه امنیت سایبری ملی[8]»و همچنین دستورالعمل‌های توسعه آموزش‌های سایبری ایجاد شده است. یکی از اهداف این مدل به‌کارگیری کارکنان با دانش فنی در امنیت سایبری است. برای رسیدن به این اهداف، سه مؤلفه در این مدل دنبال می‌گردد،۱) ایجاد ساختار امنیت سایبری کارکنان۲) مدیریت استعدادها ۳)نقش برنامه ریزی کارکنان (US Department of Homeland Security, 2014).

بلوغ منطقه تمرکز امنیت سایبری – The Cybersecurity Focus Area Maturity (CYSFAM) :

مدل CYSFAM توسط بیلگ یگیت اوزکان و دیگران[9] توسعه یافته است، این مدل برای ارزیابی قابلیت‌های امنیت سایبری و تعیین سطح فعلی بلوغ امنیت سایبری مورد استفاده قرار می‌گیرد. این مدل دارای یک ابزار ارزیابی متشکل از ۱۴۴ سؤال است که بنا به ادعای توسعه دهندگان آن، میتوان یک سازمان را در عرض چهار ساعت مورد ارزیابی قرار داد (Ozkan, 2021)

مدل CYSFAM در اوایل سال ۲۰۲۱ انتشار یافت، این مدل دارای ۱۱ سطح بلوغ است که به دو مرحله بلوغ تقسیم می‌شود، این مراحل به دو دسته فنی و سازمانی برای تسهیل درک و مدیریت بهتر گروه‌بندی می‌شوند (جدول ۳).
مدل مذکور برگرفته از استانداردهای ISO/IEC 27032, ISO/IEC 27001, ISO/IEC27033 است.

[8] CNCI (Comprehensive National Cybersecurity Initiative)
[9] Bilge Yigit Ozkan

CYSFAM	سطوح بلوغ (Maturity Level)												
ناحیه تمرکز (Focus Area)	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
فنی (Technical)													
محافظت سرور (Server Protection)					A					C	D		
کنترل‌های کاربر نهایی (End-User Controls)					A		B		C			D	
امنیت شبکه (Network security)				A		B		C			D		
امنیت نرم افزارهای کاربردی (Application Security)					A		B		C			D	
رمزنگاری (Cryptography)						A	B		C			D	
امنیت تجهیزات قابل حمل (Mobile Security)					A	B		C			D		
مدیریت آسیب پذیری‌ها (Vulnerability Management)					A	B		C			D		
سازمانی (Organizational)													
کنترل حملات مهندسی اجتماعی (Social Engineering Controls)				A		B		C			D		
مدیریت رخداد امنیت سایبری (Cybersecurity Incident Management)				A			B		C			D	
آگاهی امنیت سایبری (Cybersecurity Awareness)				A		B		C			D		E
حکمرانی امنیت سایبری (Cybersecurity Governance)		A	B					C	D				

جدول (۳) مدل CYSFAM (Ozkan, 2021)

مدل بلوغ قابلیت امنیت سایبری – Cybersecurity Capability Maturity Model (C2M2) :

مدل C2M2 توسط وزارت انرژی ایالات‌متحده توسعه یافته است. آخرین ویرایش این مدل نسخه (۲.۹) است که در جولای سال ۲۰۲۱ منتشر شده است.

این مدل در ۱۰حوزه سازمان‌دهی شده است و هر دامنه یک گروه‌بندی منطقی از اقدامات امنیت سایبری است. تمرینات در هر حوزه به اهدافی سازمان‌دهی می‌شوند که نشان دهنده دستاوردهای درون دامنه هستند(U.S Department of Energy,2021).

در ادامه، کلیه مدل‌های بلوغ امنیت سایبری و بلوغ امنیت اطلاعات که در این پژوهش مورد بررسی قرار گرفته‌اند در قالب جدول (۴) ارائه شده است.

بررسی تحقیقات پیشین نشان می‌دهد که تاکنون جنبه‌های مختلفی از امنیت سایبری و مباحث مرتبط به زیرساخت‌های سایبری مورد بررسی قرار گرفته و مدل‌های مختلفی جهت بررسی بلوغ امنیت سایبری و امنیت اطلاعات ارائه شده است، ولی مدلی مفهومی برگرفته از شاخص‌های مطروحه در مدلهای پیشین، برای بلوغ امنیت سایبری برای زیرساخت شرکت‌های ارائه دهنده خدمات پرداخت(PSP)، به عنوان یکی از زیرساخت های حیاتی کشور ارائه نشده است، این پژوهش سعی دارد به روش فراترکیب با واکاوی مدل‌های ارائه شده نسبت به تجمیع شاخص‌ها اقدام و در نهایت به احصاء شاخص‌های بلوغ امنیت سایبری و امنیت اطلاعات و ارائه مدلی مفهومی از بلوغ امنیت سایبری برای شرکت‌های ارائه دهنده خدمات پرداخت(PSP) اقدام نماید.

ردیف	نام مدل	شاخص‌های تدوین شده	سطوح/مراحل تعریف شده	سال انتشار/ آخرین ویرایش	پدید آورندگان
۱	CCSMM	شناسایی تهدیدات، اشتراک اطلاعات، تکنولوژی، آموزش، سنجش	سطح یک: ابتدایی / سطح دو: پیشرفته / سطح سه: خود ارزیابی/ سطح چهار: یکپارچه سازی/ سطح پنج: پیشرو	ژانویه ۲۰۰۷	وزارت امنیت داخلی آمریکا
۲	ISMM	نظارت بر سیستم‌ها، سیاست‌ها و روندها، امنیت اتطباق، حوادث امنیتی، معماری امنیتی، کنترل پیشگیرانه و اصلاحی	سطح یک: عدم پذیرش/ سطح دو: پذیرش اولیه/ سطح سه: پذیرش ثانویه/ سطح چهار: قابل پذیرش/ سطح پنج: پذیرش کامل	ژانویه ۲۰۱۱	Dr. Malik F. Saleh
۳	E-Government ISMM	اهداف امنیت اطلاعات، محیط خطر امنیتی، فرایندها و سیاست‌های امنیتی، فرایندهای کاهش ریسک، آگاهی	سطح یک: تعریف نشده/ سطح دو: تعریف شده/ سطح سه: مدیریت شده/ سطح چهار: تحت نظارت / سطح پنج: بهینه شده	آگوست ۲۰۱۱	Geoffrey Karokola and Others
۴	5S2IS	سیاست‌های امنیتی، سازماندهی امنیت اطلاعات، مدیریت دارایی، امنیت منابع انسانی، امنیت فیزیکی، مدیریت عملیات و ارتباطات، کنترل دسترسی، نگهداری و توسعه، کسب سیستم اطلاعاتی، مدیریت حوادث امنیتی اطلاعات، مدیریت تداوم کسب و کارانطباق	سطح یک: تعهد/ سطح دو: اصول/ سطح سه: نظارت/ سطح چهار: بهبود بخشی/ سطح پنج: استقرار	جان ۲۰۱۱	Alan Gillies
۵	GAIA-MLIS	سیاست‌ها و فرایندها، آگاهی، رخدادهای امنیتی، مدیریت دسترسی و هویت، کنترل دسترسی، امنیت فیزیکی، مدیریت شبکه، رمزنگاری داده، طبقه بندی داده	سطح صفر: بدون تضمین/ سطح یک: تضمین اولیه/ سطح دو: تضمین معین/ سطح سه: ایمنی نسبی/ سطح چهار: تضمین کامل	ژانویه ۲۰۱۴	Roger W. Coelho and Others
۶	ISFAM	مدیریت ریسک، توسعه سیاست‌ها، سازماندهی امنیت اطلاعات، امنیت منابع انسانی، انطباق، مدیریت دسترسی و هویت، توسعه امنیت نرم افزار، مدیریت حوادث، مدیریت تداوم کسب و کار، مدیریت تغییر، امنیت فیزیکی و محیطی، مدیریت دارایی، معماری	مرحله یک، طراحی/ مرحله دو، پیاده سازی/ مرحله سه، اثربخشی عملیاتی/ مرحله چهار، نظارت	ژانویه ۲۰۱۴	Marco Spruit and Martijn Röling
۷	NICE	برنامه ریزی نیروی کار، فرایند کسب و کار، مدیریت ریسک، ساختارهای حکمرانی، فعال سازی تکنولوژی	سطح محدود/ سطح در حال پیشرفت / سطح بهینه شده	آگوست ۲۰۱۷	بخشنامه امنیت ملی، توسط رئیس جمهور آمریکا جرج بوش (۲۰۰۸)
۸	CMMC	کنترل دسترسی، امنیت شخصی، مدیریت دارایی، امنیت فیزیکی، ممیزی و پاسخگویی، بازیابی، آگاهی و آموزش، مدیریت ریسک، مدیریت پیکربندی، مدیریت امنیت، شناسایی و احراز هویت، آگاهی از موقعیت، پاسخ به رویدادها، حفاظت از ارتباطات و سیستم‌ها، نگهداری، یکپارچگی اطلاعات سیستم، محافظت از رسانه	سطح یک، بهداشت اولیه سایبری/ سطح دو، بهداشت سایبری متوسط/ سطح سه، بهداشت سایبری خوب/ سطح پنج، پیشرفته	سپتامبر ۲۰۲۰	وزارت دفاع ایالات متحده
۹	CYSFAM	محافظت از سرور، کنترل‌های کاربر، امنیت شبکه، امنیت برنامه‌های کاربردی، رمزنگاری، امنیت تجهیزات قابل حمل، مدیریت آسیب پذیری، کنترل مهندسی اجتماعی، مدیریت حوادث امنیت سایبری، آگاهی امنیت سایبری، حکمرانی سایبری	سطح یک: فنی / سطح دو: سازمانی	فوریه ۲۰۲۱	Bilge Yigit Ozkan and Others
۱۰	C2M2	مدیریت دارایی، تغییر و پیکربندی، مدیریت تهدید و آسیب پذیری، مدیریت ریسک، مدیریت هویت و دسترسی، آگاهی از موقعیت، پاسخ به حوادث و رویدادها، تداوم عملیات، مدیریت ریسک شخص ثالث، مدیریت نیروی کار، معماری امنیت سایبری، مدیریت برنامه‌های امنیت سایبری	سطح: MIL0/ سطح: MIL1 / سطح: MIL2/ سطح: MIL3	جولای ۲۰۲۱	وزارت انرژی ایالات متحده

جدول (۴) مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات، مورد بررسی در این پژوهش

روش‌شناسی پژوهش

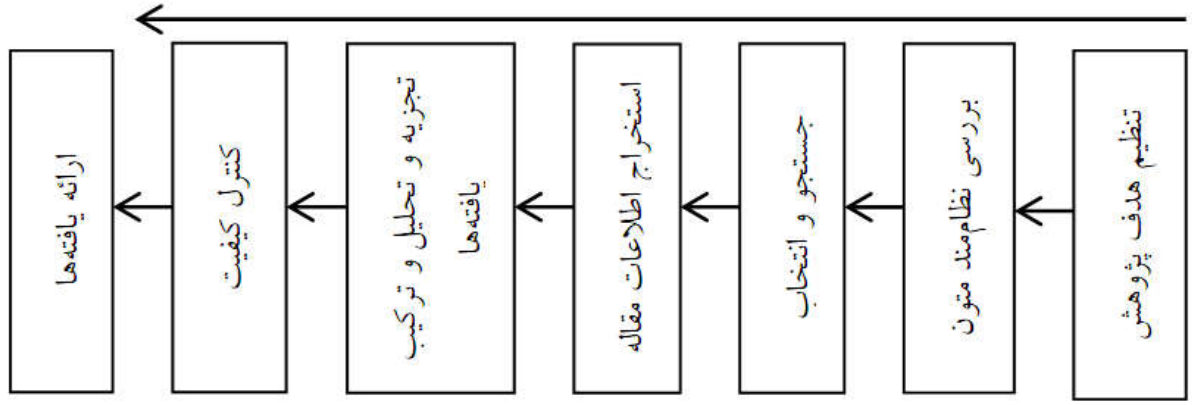
پژوهش‌های علمی از لحاظ هدف به چهار دسته‌ی کاربردی، بنیادی، تحقیق و توسعه و ارزیابی، تقسیم می‌شوند(سرمد، ۱۴۰۱) از آنجا که این پژوهش به دنبال ارائه مدل مفهومی بلوغ امنیت سایبری برای شرکت‌های ارائه دهنده خدمات پرداخت(PSP) است بنابراین از حیث هدف کاربردی و به لحاظ روش، آمیخته (کمی و کیفی) است.

در این پژوهش برای درک بهتر عوامل مؤثر در ایمن‌سازی زیرساخت‌های حیاتی و بررسی ابعاد مختلف مدل‌های بلوغ امنیت سایبری و شناسایی شاخص‌های آن و طراحی یک مدل مفهومی بلوغ امنیت سایبری برای شرکت‌های ارائه دهنده خدمات پرداخت(PSP)، از رویکرد تحقیق «فراترکیب» استفاده می‌شود. این رویکرد در مقایسه با مطالعات کیفی اولیه، به مراتب برای تولید نظریه مناسب‌تر است. این رویکرد می‌تواند در حمایت از نظریه‌های موجود، تفسیر و تشریح دقیق‌تر آن‌ها و نیز در تکمیل نظریه‌ها بکار گرفته شود(عابدی جعفری، ۱۳۹۸).

روش اجرای بخش کیفی

فرآیند انجام پژوهش با رویکرد فراترکیب یک فرآیند است که شامل مراحل گسسته‌ای است که پژوهشگر را قادر می‌سازد تا یک پرسش تحقیق مشخص را شناسایی کرده و سپس به جستجو، انتخاب، ارزیابی، خلاصه کردن و ترکیب شواهد برای پاسخگویی به سؤال تحقیق بپردازد. این فرایند با استفاده از روش‌های کیفی دقیق برای ترکیب مطالعات کیفی موجود برای ایجاد معنای بیشتر از طریق یک فرایند تفسیری انجام میشود(Erwin, 2011).

روشهای متعددی برای انجام فراترکیب پیشنهاد شده است که از بین آن‌ها الگوی هفت گام سندلوسکی و بارسو بیشترین کاربرد را دارد. در شکل زیر خلاصه این مراحل نشان داده می‌شود (Sandelowski, 2007).



شکل (۵) مراحل هفتگانه فراترکیب (Sandelowski, 2007)

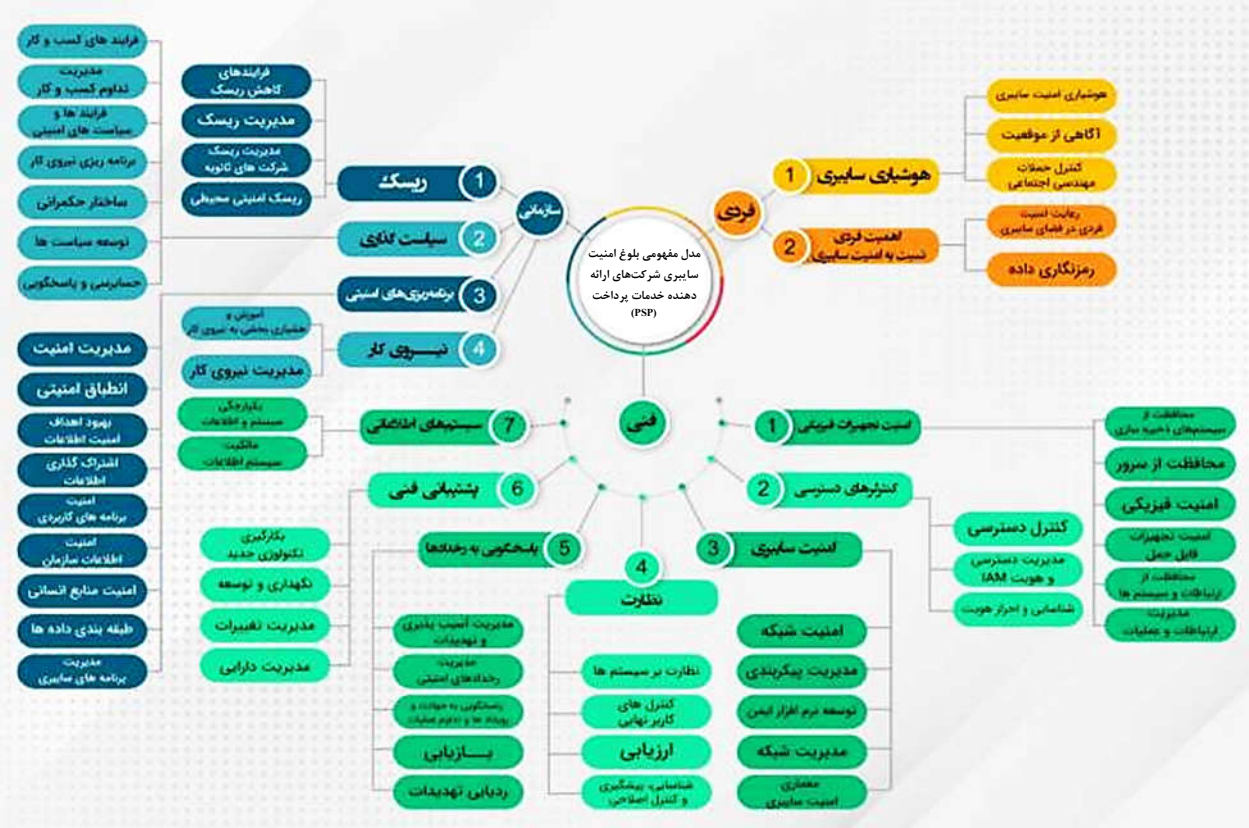
تجزیه وتحلیل داده‌ها

ابتدا با استفاده از مرور ادبیات تحقیق و پیشینه پژوهش، تعداد ۸۵ شاخص اولیه برای مدل بلوغ امنیت سایبری شرکت‌های ارائه دهنده خدمات پرداخت(PSP)شناسایی شد. بررسی دقیق این شاخص‌ها نشان می‌دهد برخی از شاخص‌های احصاء شده دارای

همپوشانی و تکراری است، بنابراین شاخص‌های تکراری حذف و در نهایت ۵۰ شاخص یکتا مشخص گردید. آنگاه مؤلفه‌های اصلی شناسایی شده (بر اساس محتوای شاخص‌ها) در قالب ۳ بعد کلی دسته‌بندی شدند. در همین راستا مؤلفه‌های «اهمیت فردی نسبت به امنیت و هوشیاری سایبری» در بعد فردی، مؤلفه‌های «مدیریت ریسک، سیاست‌گذاری، برنامه‌ریزی‌های امنیتی و مدیریت نیروی کار» در بعد سازمانی و مؤلفه‌های «امنیت تجهیزات فیزیکی، کنترلرهای دسترسی، امنیت سایبری، نظارت، پاسخگویی به رخدادها، پشتیبانی فنی و سیستم‌های اطلاعاتی» در بعد فنی قرار گرفتند.

ارائه مدل مفهومی و جمع‌بندی

برای احراز این مدل (شکل ۶)، ابتدا مبانی نظری و اسناد بالادستی بین‌المللی در حوزه امنیت سایبری مورد مطالعه قرار گرفت، سپس با انتخاب پژوهش‌های منتخب به روش فراترکیب شاخص‌های بلوغ امنیت سایبری احصاء گردید، شاخص‌های مشابه حذف و در نهایت با توجه به حوزه عملکرد و با اتکاء به مطالعات صورت گرفته در پیشینه پژوهش و مبانی نظری، ابعاد و مؤلفه‌ها تدوین و شاخص‌ها بر اساس ارتباط مفهومی در ابعاد و مؤلفه‌ها دسته‌بندی گردید و پس از آن این شاخص‌ها با ابزارهای هوش مصنوعی Chat GPT وGemini Google به اشتراک گذاشته شد، در نتیجه شاخص‌های کم‌اهمیت از نظر این هوش‌های مصنوعی حذف و شاخص‌های پیشنهادی مجدد در مرحله دوم با هوش مصنوعی Chat GPT ورژن ۴ به اشتراک گذاشته شد و این مرحله تا دستیابی به تعداد بهینه‌ای از شاخص ادامه پیدا کرد.



شکل (۶) مدل بلوغ امنیت سایبری برای شرکت‌های ارائه دهنده خدمات پرداخت(PSP)

نتیجه‌گیری و پیشنهادها

با ورود به عصر اطلاعات دیجیتال، نیازمندی شرکت‌ها و دولت‌ها به فناوری اطلاعات در جهت بهبود بخشیدن عملکردها، ارائه خدمات از راه دور و هوشمند سازی فرایندهای کسب‌وکار افزون شده است. بدین‌سان فناوری اطلاعات و امنیت سایبری و اطلاعات نیز جایگاه ویژه‌ای در عرصه دیجیتال یافته است. ازاین‌رو یکی از مهمترین خطراتی که دولت‌ها با آن روبرو هستند که می‌تواند امنیت ملی را نیز خدشه‌دار کند، حملات سایبری است. این حملات طیف گسترده‌ای از اهداف را شامل می‌شود، که اصلی‌ترین آن‌ها، آسیب رساندن به زیرساخت‌های حیاتی است. بنابراین ثبات زیرساخت‌های حیاتی در مواجهه با چنین تهدیداتی بسیار حائز اهمیت است.

بر اساس تحلیل‌های انجام گرفته و تحلیل محتوای مقالات در مجموع ۵۰ شاخص، ۱۳ مؤلفه و ۳ بعد جهت ارائه مدل مفهومی بلوغ امنیت سایبری برای شرکت‌های ارائه دهنده خدمات پرداخت(PSP) شناسایی گردید، در همین راستا مؤلفه‌های «اهمیت فردی نسبت به امنیت و هوشیاری سایبری» در بعد فردی، مؤلفه‌های «مدیریت ریسک، سیاست‌گذاری، برنامه‌ریزی‌های امنیتی و مدیریت نیروی کار» در بعد سازمانی و مؤلفه‌های «امنیت تجهیزات فیزیکی، کنترلرهای دسترسی، امنیت سایبری، نظارت، پاسخگویی به رخدادها، پشتیبانی فنی و سیستمهای اطلاعاتی» در بعد فنی قرار گرفتند.

با توجه به اینکه دستورالعمل‌های مرتبط با بلوغ امنیت سایبری باید کامل و جامع باشد به نحوی که کلیه موارد مرتبط با امنیت سایبری را در برگیرد، ازاین‌رو میتوان از این پژوهش برای تدوین دستورالعمل‌های مرتبط با بلوغ امنیت سایبری، استفاده و شاخص‌های احصاء شده در این پژوهش را مبنای تدوین این دستورالعمل‌ها قرار داد.

ارائه ایده‌های جدید جهت انجام ارزیابی سطح بلوغ امنیت

استفاده از هوش مصنوعی: هوش مصنوعی می‌تواند برای تجزیه و تحلیل داده‌های امنیتی و شناسایی الگوهای مشکوک استفاده شود.

استفاده از ابزارهای خودکار: ابزارهای خودکار می‌توانند برای جمع‌آوری اطلاعات و انجام تست‌های امنیتی مورد استفاده قرار گیرند.

استفاده از روش‌های Gamification: Gamification می‌تواند برای جذاب‌تر کردن فرآیند ارزیابی و تشویق کارکنان به رعایت نکات امنیتی استفاده شود.

مهم‌ترین محورهایی که می‌توان از نتایج این پژوهش قلمداد کرد، عبارتند از:

- شناسایی و تبیین ابعاد، مؤلفه‌ها و شاخص‌های مدل مفهومی بلوغ امنیت سایبری برای شرکت‌های ارائه دهنده خدمات پرداخت(PSP).

- امکان برنامه‌ریزی هوشمندانه توسط رگولاتور این صنعت (شرکت شاپرک) در به‌کارگیری مدل‌های بلوغ امنیت سایبری در شرکت‌های ارائه دهنده خدمات پرداخت(PSP).
- تولید ادبیات و مبانی نظری در حوزه امنیت سایبری.
- فراهم آوردن زمینه لازم برای ایجاد مواضع فعالانه در برابر حملات سایبری.
- برنامه‌ریزی برای افزایش قدرت دفاع سایبری در حوزه زیرساخت امنیت سایبری.

پیشنهادات

با توجه به اهمیت وابستگی زیرساخت شرکت‌های ارائه دهنده خدمات پرداخت(PSP) به فناوری اطلاعات، همواره تهدیدات سایبری در این حوزه وجود دارد، لذا پیشنهاد می‌شود این زیرساخت‌ها بر اساس اهمیت اولویت‌بندی گردند و برای آن‌ها دستورالعملی مشتمل بر شاخص‌های احصاء شده در این پژوهش تدوین گردد، به علاوه می‌توان با استفاده از مدل به دست آمده در این پژوهش نسبت به طراحی مدل ارزیابی بلوغ امنیت سایبری برای شرکت‌های ارائه دهنده خدمات پرداخت(PSP) اقدام کرد.

منابع

- اختری، محمد. کرامتی، محمدعلی. و موسوی، سید عبداله امین. (۱۴۰۱). مقایسه تطبیقی مدل‌های بلوغ امنیت سایبری و امنیت اطلاعات و احصای شاخصهای امنیت سایبری مشترک، فصلنامه علمی پدافند غیرعامل، ۴ (۳)، ۳۸-۲۱.
- اخوان، فاطمه. و رضا، رادفر. (۱۳۹۹) ارائه مدلی برای پایش بلوغ امنیت اطلاعات، فصلنامه رشد فناوری،۶۴ (۲)، ۵۱-۴۱.
- افشار، احمد. ترمه چی، عاطفه. گلشن، عارفه. آقائیان، آزاده. شهریاری، حمیدرضا. و سلیمانی ساجده. (۱۴۰۰). بررسی انواع راهکارهای افزایش امنیت در سیستم‌های کنترل صنعتی وزیرساخت‌های حیاتی، نشریه علمی پدافند غیرعامل، ۲، ۹-۱.
- دانایی فرد، حسن. (۱۳۸۹) تئوری سازمان: مدرن، نمادین- تفسیری و پست مدرن. چاپ دهم، تهران: انتشارات کتاب مهربان نشر.
- آذر، داود. مسلمی، حسین. (۱۴۰۱). راهبردهای قدرت سایبری ارتش جمهوری اسلامی ایران. نشریه آینده پژوهی دفاعی، ۲۷ (۷)، ۸۲-۶۳.
- اختری، محمد. کرامتی، محمدعلی. و موسوی، سید عبداله امین. (۱۴۰۲). ارائه مدل بلوغ امنیت سایبری برای زیرساخت‌های حیاتی کشور. آینده پژوهی دفاعی، ۸(۲۹)، ۱۰۱-۱۳۴.
- سرمد، زهره. بازرگان، کاوه. و حجازی، الهه. (۱۴۰۱) روش‌های تحقیق در علوم رفتاری، چاپ چهل و یکم، تهران: انتشارات آگاه.
- سعادتمند، امیر مسعود. کریمی قهرودی، محمد رضا. محمدی، حافظ. و بابک، محمد. (۱۴۰۰). تعیین شاخص‌های ارزیابی امنیت سایبری به روش مطالعه تطبیقی، نشریه علمی امنیت ملی، ۴۰ (۱۱)، ۶۶-۳۷.
- عابدی جعفری، عابد. و امیری، مجتبی. (۱۳۹۸). فراترکیب، روشی برای سنتز مطالعات کیفی، فصلنامه علمی پژوهشی روش شناسی علوم انسانی، ۲۵ (۹۹)، ۷۳-۸۷.

- کاوند، عباس. و حکیم زاده اصل، وحید. (۱۳۹۹). زیرساختهای پرخطر شناسایی، ارزیابی و طبقه‌بندی، تهران: انتشارات بوستان حمید.
- ولوی، محمدرضا. و نیک نفس، علی(۱۴۰۰). مدل بلوغ نظام رصد و پایش و هشداردهی سایبری جمهوری اسلامی ایران، فصلنامه علمی امنیت ملی، ۴۰(۱۱)، ۱۸۲-۱۵۵.
- B. Poston. (2009). Maslow's hierarchy of needs. *Surgical Technologist*, 41 (8), 347–353.
- Nye, J. Wan, J. (2006). The Rise of China's Soft Power and Its Implications for the United Statesm, *Richard Rosecrans and Gu Guoliang, Power and Restraint: A Shared Vision for the U.S.–China Relationship (New York:Public Affairs)*, 28-30.
- ITU. (2008). *Corporate Annual Report*, https://www.itu.int/osg/csd/stratplan/AR2008_web.pdf .2022-08-12.
- ISO/IEC 27032:2012. (2012). *Information technology – Securitytechniques – Guidelines for cybersecurity*, https://www.iso.org/standard/44375.html 2023-02-03.
- Y. Bilge, S. Marco. (2019). A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures. *In Springer Nature Switzerland AG Conference paper*.
- K. Bilge and Others. (2019). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness, *In international journal of critical infrastructure protection, ScinceDirect, Elsevier*,47 – 59.
- M. Ide. (2019). *cybersecurity capability maturity model for critical information technology infrastructure among nigeria financial organizations*. PhD. Thesis, Teknologi Malaysia Univ.
- M. Saleh. (2021). Information Security Maturity Model", *In International Journal of Computer Science and Security*. 316-337.
- G. Karokola, S. Kowalski & L. Yngström. (2011). Towards an Information Security Maturity Model for Secure e-Government Services: A Stakeholders View, *In Proceedings of the 5th HAISA2011, Conference*.
- P. Gillies. (2011). Improving the quality of information security management systems with ISO27000, *In the TQM Journal*, 23(4), 367–376.
- S.W. Humphrey. (1989). Managing the Software Process*, In Omega International Journals of Management Science*.
- M. Spruit and M. Roeling. (2014). ISFAM: the information security focus area maturity model, *In Proceedings of the European Conference on Information Systems (ECIS)*.
- G.B, White. (2007). The community cyber security maturity model, *In IEEE International Conference on Technologies for Homeland Security,HST*.
- US Department of Homeland Security. (2014). Cybersecurity Capability Maturity Model: Version 1.0. White paper*, Department of Homeland Security*.
- Y. Ozkan, S. Lingen, M. Spruit. (2021). The Cybersecurity Focus Area Maturity (CYSFAM) Model, *In Journal of Cybersecurity and Privacy*, 119-139.
- U.S Department of Energy. (2021). CyberSecurity Capability Maturity Model (C2M2), *Office of Cybersecurity, Energy Security and Emergency Response*.
- Erwin, E. J., Brotherson, M. J. & Summers, J. A. (2011). Understanding Qualitative Metasynthesis: Issues and Opportunities in Early Childhood Intervention Research. *Journal of Early Intervention*, 33(3):186- 200.
- Sandelowski, M. & Barroso, J. (2007) Handbook for synthesizing qualitative research. *New York: Springer conference.*