طراحی و پیاده‌سازی یک برنامه‌ریز گرافی برای هوشمندسازی انتخاب کنترل‌های امنیتی: قابل استفاده در پلیس هوشمند

مهرداد احمدی نیک[۱]، شهریار بیژنی[۲]
۱- کارشناس ارشد، ، گروه علوم کامپیوتر، دانشگاه شاهد ، تهران، ایران
mehrdad.ahmadinik@shahed.ac.ir
۲- استادیار، گروه علوم کامپیوتر، دانشگاه شاهد ، تهران، ایران
bijani@shahed.ac.ir

چکیده: در این مقاله، نتایج طراحی و پیاده‌سازی یک برنامه‌ریز هوشمند[1] برای اولویت‌بندی و انتخاب بهینه کنترل‌های امنیتی ارائه می‌شود. این برنامه‌ریز بر روی گرافی که استانداردهای مدیریت امنیت سایبری را مدل می‌نماید و در آن پارامترهای تصمیم‌گیری، شناسایی و مقداردهی شده است، عمل می‌کند. برنامه‌ریزهای هوش مصنوعی می‌توانند کارها را با در نظر گرفتن شرایط و محدودیت‌ها، اولویت‌بندی کنند. فعالیت‌هایی که توسط به‌روش[2]ها یا استانداردهای امنیتی برای بالابردن سطح امنیت شبکه‌ها و سامانه‌ها معرفی می‌شوند، کنترل امنیتی نام دارند. در این پژوهش مجموعه‌ای از کنترل‌های امنیتی برای سازمان‌های مختلف معرفی می‌شود که به ترتیب انجام دادن آنها، موجب پیشرفت صحیح، یکنواخت و بهینه در دامنه‌های مختلف امنیت سایبری می‌شود. از مهم‌ترین نوآوری این پژوهش می‌توان به خودکار شدن روند برنامه‌ریزی و هوشمند شدن اولویت‌دهی و انتخاب مدیران برای انجام کارها، اشاره کرد. برنامه‌ریز پیشنهادی بر مبنای سه الگوریتم اصلی ارسال-برچسب[3]، دکسترا[4] و امتیازدهی کمینه[5] طراحی و با زبان‌های برنامه‌نویسی سی‌شارپ و پایتون پیاده‌سازی شده و برای نمونه بر روی کنترل‌های یکی از معروف ترین مدل‌های بلوغ امنیت سایبری[6] اجرا شده است. همچنین در این مقاله، نمونه‌هایی از ادارات که به طور کلی در سازمان‌ها وجود دارند، در نظر گرفته شده و نتیجه برنامه‌ریزی هوشمند در آن‌ها، بصورت یک اولویت‌بندی از کنترل‌های امنیتی مناسب هر اداره ارائه شده است.

واژه‌های کلیدی: هوش مصنوعی، برنامه‌ریز هوشمند، مدیریت امنیت، امنیت سایبری، کنترل‌های امنیتی، بلوغ امنیت سایبری

تاریخ دریافت مقاله: ۱۴۰۰/۰۲/۲۶	تاریخ پذیرش مقاله: ۱۴۰۰/۰۴/۳۰
از صفحه ۷۹ تا ۸۹	نوع مقاله : پژوهشی
نویسنده مسئول: شهریار بیژنی	نشریه علمی فناوری اطلاعات و ارتباطات انتظامی- دوره دوم- شماره ۵ - بهار ۱۴۰۰

[1] AI Planner
[2] Best practice
[3] Push-Relabel
[4] Dijkstra
[5] Minimum Scoring
[6] C2M2 (Cybersecurity Capability Maturity Model)

۱- مقدمه

در این پژوهش برنامه‌ریزی پروژه‌ها و سازمان‌های بزرگ با برنامه‌ریزهای هوش مصنوعی بهبود یافته و مدیریت امنیت، هوشمند شده است. فعالیت‌هایی که توسط به‌روش‌ها یا استانداردهای امنیتی برای بالابردن امنیت شبکه‌ها و سامانه‌ها معرفی می‌شوند، *کنترل امنیتی* نام دارند. با توجه به اینکه پروژه‌های امنیت سایبری در سازمان‌ها یکی از موثرترین و مهم‌ترین پروژه‌ها هستند، استانداردهای مورد تحلیل برنامه‌ریز پیشنهادی، مدل بلوغ قابلیت امنیت سایبری[1] و استاندارد مدیریت امنیت ایزو ۲۷۰۰۱ انتخاب شده است. در این مقاله، نتایج تحلیل مدل بلوغ قابلیت امنیت سایبری ارائه شده است. با توجه به دسته‌بندی انواع استانداردهای امنیت سایبری (استانداردهای بین‌المللی، ملی و صنعتی) پژوهش جاری درحال حاضر در گروه استانداردهای بین‌المللی قرار می‌گیرد. البته با توجه به اینکه مدل بلوغ تدوین شده توسط مرکز مدیریت راهبردی افتای ریاست جمهوری، بر مبنای مدل بلوغ قابلیت امنیت استفاده شده در این پژوهش و بسیار مشابه این مدل است، می‌توان به سادگی با اضافه کردن مدل بلوغ افتا، این گروه را به استانداردهای ملی نیز گسترش داد. مدل‌های بلوغ امنیت سایبری رویکردی نوین در مدیریت کنترل‌های امنیت سایبری محسوب می‌شوند که امروزه در دنیا مورد استقبال بیشتری قرار گرفته‌اند. همچنین یکی از سازمان‌هایی که برنامه‌ریز می‌تواند در آن استفاده شود، نیروی انتظامی جمهوری اسلامی ایران است. با توجه به سرعت بالای محاسباتی در الگوریتم‌های هوش مصنوعی، می‌توان ترتیب پیاده‌سازی هر کنترل امنیتی در هر یک از بخش‌ها یا رسته‌های تخصصی‌تر این سازمان را نیز با این برنامه‌ریز به دست آورد. در ادامه برنامه‌ریز بر روی نمونه‌هایی از ادارات که به طور کلی در هر نوع سازمانی وجود دارند، اجرا شده است.

در این حوزه، به طور مستقیم پژوهش مشابهی انجام نشده است، اما پژوهش‌های مرتبط با برنامه‌ریزی مفاهیم امنیت سایبری مورد بررسی قرار گرفته است.

۲- پیشینه پژوهش

یکی از نزدیک‌ترین مقاله‌هایی که می‌تواند الهام‌بخش پژوهش جاری باشد مقاله [۱] است. این مقاله با روش برنامه‌ریزی کلاسیک فعالیت‌هایی را تولید می‌کند که به مدیران شبکه در تحلیل آسیب پذیری‌ها، کمک می‌کند.

بادی و همکاران در مقاله [۱] کاربرد برنامه‌ریز هوشمند در مفهوم امنیت شبکه را به خوبی نشان می‌دهد، همانطور که پژوهش جاری برنامه‌ریز هوشمند را در مفهوم امنیت سایبری بکار می‌برد. البته الگوریتم برنامه‌ریزی در مقاله مورد بررسی قرار نگرفته است و این درحالی است که در پژوهش جاری الگوریتم جدیدی طراحی شده است.

دوبسکی در [۲] به معرفی معیارهای تصمیم گیری به منظور کاهش ریسک و بررسی چندین مدل و استاندارد پرداخته است. این پژوهشگر مدل امنیتی ان‌آی‌اس‌تی[2] را بررسی کرده و در آخر سوالاتی درباره مورد آزمایش قرار دادن کنترل‌های امنیت سایبری به صورت دستی و یا با ابزار، مطرح می‌کند.

مقاله فایست و بروکین [۳] نیز از نظر اینکه تنها به بررسی کاهش ریسک و بودجه می‌پردازند، زیر مجموعه مقالات بالا قرار می‌گیرد. همچنین مقالات دیگری مانند [۴] وجود دارند که با کمی‌سازی و اعمال ریاضی سعی بر استخراج مدل‌هایی برای امنیت اطلاعات و ریسک سازمانی دارند. در پژوهش جاری این مدل‌سازی با گراف انجام شده است تا با برنامه‌ریز هوش مصنوعی همخوانی بهتری داشته باشد.

حاجم و همکاران در [۵] به موضوع امنیت در سازمان‌ها با رویکرد مسئله تخصیص منابع می‌پردازد. در این مقاله، یک الگوریتم مبتنی بر جستجوی‌هارمونی برای حل مدل تصمیم گیری تخصیص منابع به صورت پویا پیشنهاد شده است. این رویکرد با یک الگوریتم ژنتیک مقایسه شده و نتایج خوبی را ارائه کرده است. البته تعداد معیارهای مورد بررسی برای تصمیم‌گیری کافی بنظر نمی‌رسد.

میلوسویک و همکاران در دو مقاله [۶] و [۷] پیرامون مسئله نزدیک‌تری به کار جاری بحث می‌کنند. این مقالات به طور کلی به چگونگی تخصیص تعداد زیادی از اقدامات امنیتی با بودجه محدود و به منظور به حداقل رساندن خطرات کلی حملات سایبری، پرداخته‌اند. همچنین با بررسی این موضوع که این مسئله یک مسئله ان‌پی سخت[3] است به دنبال راه حل‌های با زمان چند جمله‌ای آن هستند. با درنظر گرفتن این‌که بودجه یکی از چندین پارامتر مهم تصمیم‌گیری در سازمان‌هاست، روش‌های الگوریتمی و هدف مقالات میلوسویک و همکاران مشابهت‌هایی با مقاله جاری دارد.

[1] C2M2

[2] NIST

[3] NP-hard

در [۸] ، رازک و همکاران با توجه به تهدیدات و ریسک‌های متعددی که در زنجیره تامین وجود دارد، یک روش برنامه‌ریزی با تمرکز بر مدیریت ریسک ارائه کرده‌اند. پژوهش آن‌ها بیشتر بر زمان انجام یک کار تکیه داشته و با شبیه سازی توسط روش مونت کارلو آن را محاسبه می‌کند. این پژوهش با در نظر گرفتن معیارهای زمان و میزان ریسک در حوزه زنجیره تامین، به صورت غیر هوشمند تا حد خوبی به مدیران پروژه‌ها کمک می‌کند. زنجیره تامین یکی از حوزه‌های ده‌گانه در این مقاله و معیارهای زمان و میزان ریسک دو مورد از چندین معیار تصمیم‌گیری پیشنهاد شده در مقاله جاری برای کمک به تصمیم‌گیری مدیران سازمان‌هاست.

پوررضا در [۹] به موضوع امنیت در سازمان‌های دارویی پرداخته است. در این پژوهش با تکنیک ای‌اچ‌پی[1] از متخصصان حوزه داروسازی و امنیت اطلاعات نظرخواهی شده و تهدیدات و آسیب پذیری‌های مهم امنیتی در این نوع سازمان‌ها شناسایی شده است. پژوهشگر با اولویت بندی آن‌ها به دو روش، تهدیداتی که ریسک بیشتری دارند را معرفی کرده و کنترل‌ها و تدابیر لازم جهت برطرف کردن آن‌ها را پیشنهاد نموده است. در این پایان نامه از استانداردهای مدیریت کنترل‌های امنیتی استفاده نشده و همچنین اولویت بندی با دو روش غیر هوشمند انجام شده است.

خاک بیز [۱۰] به استخراج پارامترهای مهم همسوسازی اهداف و عملکرد امنیت اطلاعات پرداخته است. با توجه به اطلاعات جمع شده و تحلیل آن، این پژوهش ۱۰ معیار اصلی و ۳۲ زیرمعیار را معرفی می‌کند که مدیران سازمان‌ها و متخصصان امنیت اطلاعات توسط آن بتوانند راه حل‌های بهتری در مدیریت امنیت اطلاعات را عملی کنند.

این پژوهش با استخراج معیارها تا حد خوبی نقشه راه را برای متخصصان امنیت اطلاعات روشن کرده است ولی متخصصین باید با در نظر گرفتن سازمان هدف کنترل‌های یک استاندارد خاص را با اولویت انجام به مدیران سازمان به صورت تجربی پیشنهاد دهند. همچنین مفاهیم بلوغ امنیت موضوع بررسی آن نبوده است.

موسوی در [۱۱] به مطالعه روی کنترل‌های استانداردهای معرفی شده پرداخته است و با اولویت بندی آن‌ها به سازمان‌ها مسیر عملکرد بهتر را پیشنهاد می‌کند. این پژوهش نیز با تکنیک ای‌اچ‌پی فازی، شدت ریسک‌ها و احتمال وقوع آن‌ها را جمع آوری کرده و با محاسبه حاصلضرب این دو اولویت هر ریسک را تعیین می‌کند.

پژوهش [۱۱] اولویت بندی را بر اساس محاسبه ریسک و با فرمولی از حاصلضرب دو پارامتر مربوط به ریسک انجام داده است. روش فوق روش آماری محسوب شده و رویکرد متفاوتی نسبت به روش‌های هوشمند مورد استفاده در مقاله جاری دارد. همچنین پارامتر ریسک، تنها یکی از چند عامل مهم برای اولویت بندی کارها از دید مدیران، شناخته می‌شود.

۳- تعریف و توضیح مفاهیم

۳-۱- برنامه‌ریزی

برنامه‌ریزی یکی از مهم‌ترین قدم‌هایی است که مدیران سازمان‌ها باید قبل از انجام هر کاری انجام دهند. همچنین در سازمان‌ها و پروژه‌های بزرگ ممکن است برنامه‌ریزی در هر مرحله و با توجه به خروجی مرحله قبل تغییر کند. یک برنامه‌ریز خوب باید خصیصه‌ها و ویژگی‌های تاثیرگذار بر پروژه را بشناسد و با کمک آن پارامترهای برنامه‌ریزی را تعریف کند. این تعریف باید به گونه ای باشد که هیچ دو پارامتری یک ویژگی را توضیف نکرده و همه پارامترها کل جوانب مسئله را مورد بررسی قرار دهند. اولویت بندی انجام کارها به روش‌های مختلف می‌تواند زمان کل پروژه را تا چند برابر جابجا کند. حتی ممکن است حالاتی از ترتیب انجام کارها باعث شود یک پروژه هیچ‌گاه به سرانجام نرسد، در نتیجه منابع مالی و نیروی انسانی هزینه شده را هدر بدهد.

پروژه‌های امنیت سایبری که هریک به هدف امن‌سازی بیشتر سازمان‌ها تعریف می‌شوند نیز باید برنامه‌ریزی و اولویت بندی شوند. هر پروژه از چند بخش و هر بخش از فعالیت‌ها و زیرفعالیت‌هایی تشکیل شده است که در صورت انجام ندادن یا اشتباه انجام دادن هرکدام، ممکن است نه تنها باعث پیشرفت سطح امنیت سازمان نشود، بلکه روزنه‌ی نفوذی ایجاد کرده و سازمان را آسیب‌پذیرتر کند. در پروژه‌های امنیت سایبری خیلی از ویژگی‌های تصمیم‌گیری به صورت کیفی یا بازه‌ای می‌باشند. این موضوع سبب شده است تا پیش از مرحله برنامه‌ریزی در مورد کاربرد امنیت سایبری، مرحله کمی‌سازی داده پارامترها انجام شود. این کمی‌سازی باید به گونه‌ای باشد که از دقت مقادیر تصمیم‌گیری کاسته نشود.

۳-۲- برنامه‌ریز هوش مصنوعی

یکی از حوزه‌های هوش مصنوعی، برنامه‌ریزی است. مجموعه ای از الگوریتم‌ها، در این حوزه وجود دارند که وظیفه آن‌ها پیشنهاد کردن

[1] AHP

یک دنباله از کارها است که با انجام دادن بـه ترتیـب آنهـا، مسـئله در حالت بهینه به پاسخ خود می‌رسد. برنامه‌ریزهای هوشمند اصـولا روی گرافی کار می‌کنند که دوحالت اولیه مسئله و هـدف دو راس شـروع و پایان آن، حالات دیگـری ممکـن اسـت رخ بدهـد راس‌هـای میـانی و اعمالی که قابل انجام شدن هستند یـال‌هـای بـین راس‌هـا را تشـکیل می‌دهند. به این گراف، فضای حالت می‌گویند. در صورتی که در هر دو اجرا از الگوریتم برنامه‌ریز، مسیر پیشنهاد شده بـا نتیجـه اجـرای قبـل متفاوت باشـد، ایـن الگـوریتم را غیرقطعـی مـی‌نامنـد. الگـوریتم‌هـای غیرقطعی در محیط‌های غیرقطعی بهتر عمل می‌کنند و مـی‌تواننـد بـا درک محیط در هر قدم اجرا، تصمیم نزدیک تری به واقعیت را بگیرند. همچنین با توجه به دسـته‌بنـدی مسـائل فراابتکـاری[1]، ایـن مسـئله و الگوریتم پیشنهاد شده در دسته الگوریتم‌های مبتنی بر جمعیت، الهـام گرفته از طبیعت، بدون حافظه و غیرقطعی قرار می‌گیرد.

۳-۳- مدل بلوغ امنیت سایبری

مدل بلوغ یک متدولوژی برای سنجش وضع بلوغ سازمان‌هاسـت. ایـن مدل‌ها با سوالاتی که در دامنه‌های مختلف امنیت سایبری می‌پرسـند، می‌توانند حالت فعلی سازمان را پیدا کرده و قدم بعـدی را بـه مـدیران پیشنهاد دهند. برای برداشتن قدم و انجام فعالیت در هر پروژه بـزرگ، دانستن وضعیت فعلی و جایی که سازمان ایستاده است، می‌تواند یکـی از مهم‌ترین کارهایی باشد که از هدررفت منابع، مالی، انسانی یا زمانی، جلوگیری کند. مدل بلوغ قابلیـت امنیـت سـایبری[2]، بـه منظـور درک وضعیت فعلی امنیـت در سـازمان، دارای ۳۱۲ کنتـرل امنیتـی در ۱۰ دامنه مختلف بوده که اسامی‌دامنه‌ها در جدول (۱) آمده است. ترتیـب دامنه‌ها، کدها و عنوان کنترل‌ها از مرجع [۱۲] آمده است. مدل بلـوغ مشابهی توسط مرکز مدیریت راهبردی افتای ریاسـت جمهـوری ارائـه شده است که با تغییراتی جزئی می‌تواند جایگزین مـدل بلـوغ قابلیـت امنیت سایبری در این پژوهش شود.

جدول (۱): اسامی دامنه‌های مدل بلوغ امنیت سایبری C2M2

نام فارسی دامنه	مخفف انگلیسی
مدیریت ریسک	RM
مدیریت دارایی، تغییر و پیکربندی	ACM
مدیریت دسترسی و هویت	IAM
مدیریت آسیب پذیری و تهدید	TVM
آگاهی از وضعیت	SA
ارتباطات و به اشتراک گذاری اطلاعات	ISC
پاسخ به رویداد و رخداد، تداوم عملیات	IR
مدیریت روابط برون‌سازمانی و زنجیره تامین	EDM
مدیریت منابع انسانی	WM
مدیریت برنامه امنیت سایبری	CPM

کارشناسان طراح این مدل بلوغ، برای هر کنترل آن یـک سـطح بلـوغ تعیین کرده‌اند، بدین گونه که فعالیت‌های ساده‌تر و ضروری‌تر در سطح بلوغ ۱ و کارهای پیچیده تر، مـدیریتی‌تـر و در سـطح اسـتراتژیک، در سطح بلوغ ۳ قرار دارند. مدیران سازمان‌ها می‌توانند با اسـتفاده از ایـن سطوح بلوغ فعالیت‌های ساده‌تـر را سـریع‌تـر انجـام دهنـد و از انجـام کارهای سطح بالاتر تا زمـانی کـه فعالیـت سـطح پـایینی وجـود دارد، خودداری کننـد. همچنـین بـا بررسـی وضـعیت فعلـی سـازمان خـود می‌توانند فعالیت‌هایی را در نقشه راه خود قرار دهند که از دامنه‌هـایی انتخاب شده باشد که کمتر سازمان به سمت آن‌ها رفته است. اسـتفاده از این متدولوژی باعث می‌شود اصطلاحا سازمان به صورت یکنواخت و متناسب با وضعیت خود به بلوغ برسد. نسخه جدیدتری از این مدل به تازگی منتشر شده است که کنترل‌ها و نام دامنه‌ها در آن تغییر یافته و از نظر امنیتی بهبود بخشیده شده است که در [۱۵] آمده است.

۴- طرح مسأله

همانطور که پیش‌تر بیان شد، مدیران برای انجام یک پروژه بلوغ امنیت سایبری به منظور ارتقاء سطح بلوغ امنیتی در سازمان‌ها، لازم است تـا ابتدا وضع امنیت سازمان را به هر روشی و با کمک پرسش‌های مدل‌ها و استانداردهای مدیریت امنیت مانند مدل بلوغ قابلیت امنیت سایبری، ارزیابی نموده و سپس برای بالا بـردن امنیـت، نقشـه راهـی را از روی مدل بلوغ طراحی کنند. این روند شامل انتخاب کنترل‌های انجام نشده این مدل است. به منظور ارزیابی بلوغ سازمان، می‌توان از سـامانه‌هـایی

[1] Meta-Heuristics
[2] C2M2

مانند ای‌اس‌پی[1] یا سامانه برنامه‌ریزی امنیت سازمانی استفاده کرد[۱۳].

استفاده از سطوح بلوغی که مدل بلوغ قابلیت امنیت سایبری برای هر کنترل خود معرفی کرده است، برای انتخاب یک کنترل کافی نیست. مدیران نمی‌توانند به راحتی کنترل‌ها را به ترتیب انتخاب کنند. مدیران از اهمیت هر یک از کنترل‌های هم سطح باخبر نیستند. همچنین با توجه به زیاد بودن معیارهای تصمیم گیری و نزدیک بودن ارزش کنترل‌ها، کارشناسان نیز به طور دستی نمی‌توانند به سرعت و راحتی کنترل‌ها را اولویت بندی کنند.

بسیاری از کنترل‌ها از نظر مفهومی، به هم وابسته بوده و بر خلاف هم سطح بودن، پیش‌نیاز یکدیگر محسوب می‌شوند. مدیران در مرحله برنامه‌ریزی متوجه این پیش‌نیازی نمی‌شوند و این اختلاف‌ها حین انجام پروژه خود را نشان می‌دهند. در صورتی که مدیران و کارشناسان متوجه این پیش‌نیازی نشوند، حین انجام فعالیت‌ها مشکلات بزرگی ایجاد می‌شود. پیامدهای این ناآگاهی ممکن است به توقف دائمی پروژه امنیتی تعریف شده توسط مدیر در سازمان، یا تحمیل هزینه‌های زمانی و مالی بسیار زیاد برای سازمان منجر شود.

۵- راه‌حل پیشنهادی

با توجه به توضیح ارائه شده درباره برنامه‌ریز هوش مصنوعی، یکی از راه حل‌های کارا برای برنامه‌ریزی سریع و دقیق در سازمان ها، استفاده از برنامه‌ریزهای هوش مصنوعی است. حالت اولیه این برنامه‌ریز می‌تواند وضعیت جاری بلوغ امنیت سازمان و حالت هدف، وضعیت مطلوب امنیت از نظر مدیران عالی و فنی باشد.

از آنجایی که مدل‌های بلوغ امنیت سایبری به دنبال ارزیابی وضعیت فعلی امنیت در سازمان‌ها می‌باشند، پس یکی از ورودی‌های برنامه‌ریز باید خروجی مرحله ارزیابی امنیتی سازمان باشد.

ورودی دیگر برنامه‌ریز، مقادیر لازم برای تصمیم‌گیری انتخاب کنترل‌ها است. به منظور انتخاب بین کنترل‌ها ۷ معیار تخصصی علاوه بر سطح بلوغی که مدل بلوغ قابلیت امنیت سایبری به هر کنترل اختصاص داده است تعیین شده است. این معیارها با استفاده از رویکرد مدیریت ریسک به دست آمده است که به طور مثال به استاندارد مهاری می‌توان اشاره کرد. عناوین و واحد هر معیار را می‌توانید در جدول (۲) مشاهده کنید. مقادیر متناسب با هر معیار به ازای هر کنترل، توسط کارشناسان متخصص بلوغ امنیت سایبری مقداردهی شده است.

جدول (۲) : معیارها و واحد آن‌ها

معیار	واحد
حداقل زمان مورد نیاز برای انجام	ماه
نیروی کار عادی	نفر ماه
نیروی کار متخصص	نفر ماه
میزان عدم پذیرش (مدیران یا کارمندان)	بازه ۰ تا ۲ به معنی میزان مقاومت
میزان تاثیر(میزان کاهش ریسک)	بازه ۱ تا ۳ به معنی میزان تاثیر
هزینه مستقیم (تجهیزات و...)	بازه ۰ تا ۲ به معنی میزان هزینه
وابستگی به همکاری شخص ثالث (تامین کنندگان یا مدیران بالادستی)	بازه ۰ تا ۲ به معنی میزان وابستگی

ورودی دیگر برنامه‌ریز، اطلاعات پیش‌نیازی‌های منطقی این کنترل‌ها است. به طور مثال کنترل با کد IAM-1a باید پیش‌نیاز کنترل با کد IAM-1c درنظر گرفته شود. کنترل با کد IAM-1a بیان می‌کند "به کارکنان و سایر موجودیت‌ها که نیازمند دسترسی به دارایی‌ها هستند، شناسه‌های هویتی منحصر به فرد تخصیص دهید." و در کنترل با کد IAM-1c بیان شده است "شناسه‌های هویتی که دیگر نیازی به آن‌ها نیست را باطل کنید.". واضح است اگر شناسه ای تخصیص داده نشده باشد، نمی‌تواند باطل شود. این درحالی است که سطح بلوغ هر دو کنترل، از سوی مدل بلوغ، ۱ معرفی شده است، اما وابستگی معنایی بین آن‌ها وجود دارد. خروجی برنامه‌ریز، لیستی از کنترل‌هاست که باید به ترتیب انجام شوند. یکی از نمونه‌های خروجی برنامه‌ریز در جدول (۳) آمده است.

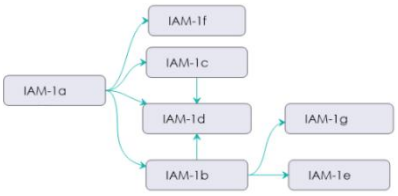
جدول (۳) : پنج ردیف اول از خروجی برنامه‌ریز برای دامنه مدیریت دسترسی و هویت برای نمونه

عنوان	کد کنترل	سطح بلوغ[2]	اولویت
دسترسی‌هایی که دیگر مورد نیاز نیست را باطل کنید.	IAM-2c	۱	۱
الزامات دسترسی تعریف کنید. (الزامات دسترسی متناسب با دارایی‌ها هستند. این الزامات، دسترسی مجاز موجودیت‌ها به دارایی‌ها، محدودیت‌های دسترسی و ملاحظات تایید هویت را تعیین می‌کنند).	IAM-2a	۱	۲
به کارکنان و سایر موجودیت‌ها (به عنوان مثال دستگاه‌ها و سامانه‌ها) که نیازمند دسترسی به دارایی‌ها هستند، شناسه‌های هویتی منحصر به فرد تخصیص دهید.	IAM-1a	۱	۳
شناسه‌های هویتی که دیگر نیازی به آن‌ها نیست را باطل کنید.	IAM-1c	۱	۴
دسترسی‌ها را بر اساس نیازمندی‌های تعیین شده، اعطا کنید.	IAM-2b	۱	۵

[1] ESP (Enterprise Security Planning)

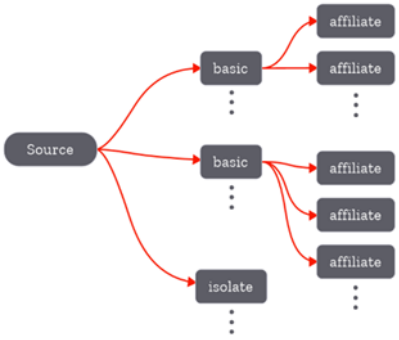
[2] MIL (Maturity Indicator Level)

در صورتی که بخواهیم برنامه‌ریز را روی مفاهیم توضیح داده شده پیاده سازی کنیم، لازم است این مفاهیم به شکل فرمال مدل شوند. مدلسازی در نظر گرفته شده به شکل گراف بوده تا با مفهوم برنامه‌ریز بهتر تطبیق داده شود. کنترل‌های امنیتی راس‌های گراف و عمل انجام دادن هر کنترل یک یال است. توجه شود این گراف ساختار داده ای است که برنامه‌ریز با آن کار می‌کند و با گراف فضای حالت متفاوت است. بین هر دو راس از گراف تنها زمانی می‌تواند یک مسیر وجود داشته باشد که قواعد پیش نیازی بین آن‌ها رعایت شود. به طور نمونه در مثال قبل از راس با کد IAM-1a یک مسیر به راس با کد IAM-1c موجود است. نمونه ای از این گراف را می‌توان در شکل (۱) مشاهده کرد.



شکل (۱) : بخشی از گراف مدل شده دامنه مدیریت هویت و دسترسی توسط پیش‌نیازی

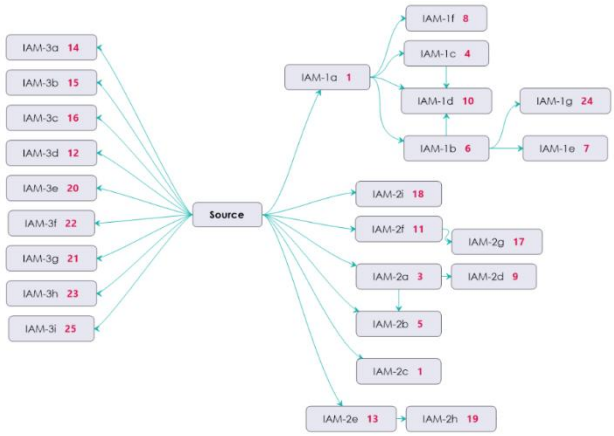
با توجه به اینکه راس‌هایی در این گراف موجود است که هیچ پیش‌نیازی ندارند، همه آن‌ها را به یک راس مجازی متصل کرده و نام آن را مبدا می‌گذاریم. این کار به این دلیل انجام می‌شود که برای شروع بین همین راس‌های بدون پیش‌نیاز، برنامه‌ریز تصمیم گیری کند. در صورتی که این راس‌های ردیف اولی خود پیش‌نیاز راس یا کنترل دیگری نباشند، آن را راس ایزوله می‌نامیم (شکل (۲)).



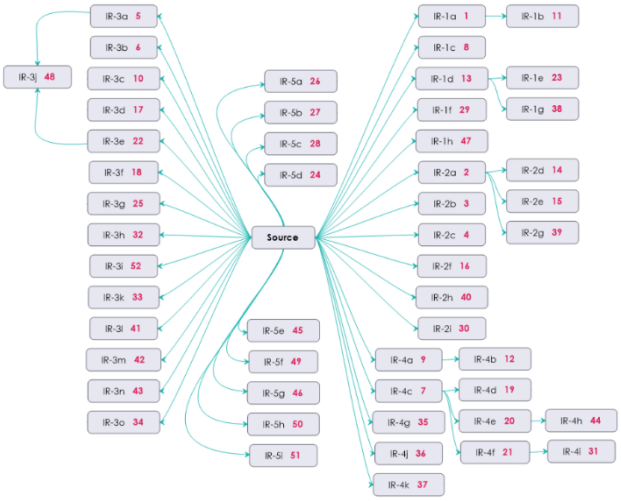
شکل (۲) : نحوه ارتباطات در گراف نمونه

برنامه‌ریز در گراف فضای حالت به دنبال یک مسیر از حالت اولیه به حالت هدف است. توجه شود این گراف موازی با حرکت برنامه‌ریز روی گراف مدل شده ساخته شده و در پایان بهترین مسیر را پیدا می‌کند، اما برنامه‌ریز در گراف مدل شده به دنبال ملاقات یک سری راس است تا بتواند پس از هر ملاقات، آن راس را به مدیر پیشنهاد دهد. پس در هر حرکت، برنامه‌ریز باید تلاش کند بهترین راس همسایه خود را برگزیند. با توجه به اینکه این حرکت، عمل انتخاب بهترین است و برنامه‌ریز بهترین تصمیم خود را می‌گیرد و به راس دیگری نقل مکان می‌کند، می‌توان الگوریتم‌های بیشینه جریان[1] را روی آن اعمال کرد. از این رو در این برنامه‌ریز، از الگوریتم ارسال-برچسب که به عنوان یکی از مشتق‌های بهینه الگوریتم ارسال پیش‌جریان[2] شناخته می‌شود، استفاده شده است. همانطور که *آقای طلایی و همکاران* در [۱۴] با پیاده سازی مناسبی از ارسال-برچسب توانسته اند به صورت بهینه ای نسبت به دیگر الگوریتم ها، مسئله خود را حل کنند. تفاوت مهمی‌که این مسئله را از بیشینه جریان متفاوت می‌کند، اینست که در این مسئله پس از اینکه انتقال از راس ۱ به راس ۲ انجام شد، بدین معنی که راس ۱ پیش‌نیاز ۲ بوده و ۱ انجام شده است، برنامه‌ریز راس ۲ را به مدیر پیشنهاد می‌دهد، اما همچنان می‌تواند به راس ۱ بازگردد. زیرا ممکن است راس ۳ ای وجود داشته باشد که راس ۱ پیش‌نیاز آن هم بوده و می‌تواند در کاندیداهای بعدی انتخاب برنامه‌ریز انتخاب شود. پس در تکرار بعدی، علاوه بر همسایه‌های راس ۲، همسایه‌های ملاقات نشده راس ۱ نیز به عنوان کاندیدا در نظر گرفته می‌شوند. در نتیجه حرکت روی گراف با الگوریتم ارسال-برچسب همچنان در نتیجه به یک مسیر می‌رسد که آن مسیر بیشینه جریان از راس مبدا به مقصد است، اما حرکت با الگوریتم برنامه‌ریز روی گراف مدل شده در نهایت به یک درخت می‌رسد. این درخت یک زیرمجموعه از گراف است و هر یک از راس‌های آن که همان کنترل‌های امنیتی هستند برچسب شماره اولویت خورده اند. شکل (۳) نمونه ای از درخت دامنه مدیریت دسترسی و هویت و شکل (۴) نمونه ای از دامنه پاسخ به رخدادهای امنیتی است.

[1] Maximum Flow
[2] Preflow Push



شکل (۳) : گراف اولویت بندی شده دامنه مدیریت دسترسی و هویت



شکل (۴) : گراف اولویت بندی شده دامنه پاسخ به رخداد

۶- پیاده‌سازی مدل پیشنهادی

ابتدا کنترل‌هایی که انجام شده است و به عنوان ورودی به برنامه داده شده است، در برنامه‌ریز به عنوان انجام شده در نظر گرفته می‌شود. سپس برنامه‌ریز شروع به حرکت از راس مبدا می‌کند و شروع به ساختن گرافی از حالات ممکن می‌کند. این عملیات توسط الگوریتم دکسترا و ملاقات همسایه‌های همه راس‌های با برچسب "انجام شده" عملی می‌شود. نکته قابل توجه این‌است که وقتی یک راس با راس دیگر همسایه است که مسیری بین آن‌ها وجود داشته باشد. بدین معنی که یکی پیش‌نیاز دیگری است. پس اگر یک راس پیش‌نیاز چندین راس باشد و برچسب آن به "انجام شده" تغییر کند، در تصمیم گیری بعدی تمام کنترل‌هایی که این راس پیش‌نیاز آن‌ها بوده، مورد بررسی دکسترا و در نتیجه مورد بررسی برنامه‌ریز قرار می‌گیرند.

در هر دور برنامه‌ریزی پس از اینکه راس‌های قابل انجام با توجه به عدد سطح بلوغ آن‌ها شناسایی شدند، برنامه‌ریز آن‌ها را راس‌های فعال[1] نامیده و وارد ماژول امتیازدهی می‌کند. یک قانون مبتنی بر مدل بلوغ قابلیت امنیت سایبری در برنامه‌ریز وجود دارد که تا وقتی راسی با سطح بلوغ ۱ وجود دارد که پیشنهاد نشده است، برنامه‌ریز نباید سراغ راس‌های با سطوح بلوغ ۲و۳ برود و همینطور اگر راسی با سطح بلوغ ۲ معرفی نشده است، برنامه‌ریز سراغ راس‌های با سطح بلوغ ۳ نرود.

ماژول امتیازدهی با بررسی هر هفت ویژگی مقدار دهی شده، راس‌های فعال را امتیازدهی می‌کند. شایان توجه است که دو پارامتر عدد سطح بلوغ و پیش‌نیازی مفهومی، پیش‌تر در انتخاب این راس‌ها در نظر گرفته شده است. روند امتیازدهی بدین صورت است که هر راس به ازای هر ویژگی ایده آل خود، امتیازی به آن اضافه می‌شود. ویژگی ایده آل نیز بسته به معیارهای تصمیم گیری، می‌تواند بیشینه بودن یا کمینه بودن معنی دهد. به طور مثال برای معیار میزان کاهش ریسک، ایده آل بیشینه بودن است. به بیان دیگر کنترلی بهتر است که با انجام آن ریسک در سازمان بیشترین میزان کاهش خود را داشته باشد. اما برای معیار هزینه مستقیم ایده آل کمینه بودن است. بدین معنی که کنترلی بهتر است که کمترین هزینه مستقیم برای انجام آن لازم باشد. امتیازی که به هر راس اختصاص می‌یابد عدد نرمال شده از اهمیت دامنه‌ای است که آن کنترل در سازمان هدف دارد. این لیست اهمیت‌ها پیش از برنامه‌ریزی، از مدیران سوال می‌شود. فرض کنید در سازمانی مانند بایگانی پرونده‌ها، اهمیت دامنه هویت و دسترسی خیلی بالا باشد ولی دامنه مدیریت روابط برون سازمانی اهمیتی نداشته باشد. مسلم است در این سازمان کنترل‌های دامنه روابط برون سازمانی هرچند هم که از معیارهای بهینه‌ای برخوردار باشند، باید امتیاز کمتری نسبت به کنترل‌های دامنه هویت و دسترسی داشته باشند. این روند امتیازدهی، نتیجه‌ی برنامه‌ریز را متناسب و قالب سازمان هدف می کند.

پس از امتیاز گرفتن همه راس‌های فعال، ماژول دیگری اقدام به انتخاب راس‌های با امتیاز بالا می‌کند. بدین صورت که فرض کنید در یک اقدام انتخاب، دنباله امتیازها به شکل ۳۰، ۳۰، ۲۹ ، ۲۹، ۲۶، ۱۲ باشد. در این انتخاب راس‌های با امتیاز ۳۰ بیشینه بوده و انتخاب می‌شوند.

با الهام از الگوریتم ارسال-برچسب پس از انتخاب این راس‌ها و اولویت گرفتن هر کدام، برچسب کنترل متناظر با آن‌ها به انجام شده تغییر

[1] Active Nodes

کرده و در دور بعدی الگوریتم دوباره راس‌های فعال جدیدی شناسایی می‌شوند.

در هر دور انتخاب بررسی می‌شود که اگر تمام راس‌های انجام نشده، معرفی شده باشد، برنامه‌ریز متوقف شود، در غیر اینصورت تا رسیدن به انتها، برنامه‌ریز همین روند را تکرار می‌کند.

روند انجام الگوریتم به طور خلاصه در شکل (۵) آمده است.

```
Least_MIL_Node <- identify nodes with least existing MIL
Active_Nodes <- use Dijkstra to determine active nodes list in Least_MIL_Node
Best_Node <- execute Minimum_Scoring on Active_Nodes list and choose
add Best_Node to Plan list
change state of Best_Node to done
go to step 1 while has unplanned node
```

شکل (۵) : شبه کد الگوریتم برنامه‌ریز

۷- جمع‌بندی و نتیجه‌گیری

با هوشمند سازی تصمیم‌گیری و برنامه‌ریزی، نه تنها سرعت بلکه دقت انجام کارها نیز به شکل چشم‌گیری افزایش می‌یابد. بسیاری از پروژه‌های بزرگ که به معیارهای متفاوتی وابسته بوده و برنامه‌ریزی برای آن‌ها مشکل و بعضا نشدنی است، با هوش مصنوعی و استفاده از برنامه‌ریزهای هوشمند به یکی از کارهای قابل انجام در سازمان‌ها تبدیل می‌شوند.

مدیر یک سازمان لازم است با دیدی که به مسائل و اولویت‌های سازمان خود دارد، با مقداردهی هفت ویژگی مرتبط با پروژه‌های امنیت و همچنین دو ویژگی مختص مدل یا استاندارد انتخاب شده که در روند مدل‌سازی معرفی شد، می‌تواند یک نقشه راه سفارشی‌سازی شده از برنامه‌ریز دریافت کرده و بسیاری از چالش‌ها و سردرگمی‌های پروژه‌های امنیت سایبری را هموار سازد و ترتیب عملیاتی متناسب با سطح بلوغ سازمان را تبیین کند.

با وصل کردن همه راس‌های مجازی مبدا هر دامنه، به یک راس مجازی با نام مبدا کل، و اجرای یکبار برنامه روی آن، همه کنترل‌ها را می‌توان یکجا برنامه‌ریزی کرد. این کار نسبت به اجرای جداگانه‌ی برنامه‌ریز روی هر یک از دامنه‌ها این مزیت را دارد که، مدیر می‌تواند دید گسترده‌تری نسبت به انجام کارها داشته باشد. این دید سطح بالا به مدیریت کلان پروژه‌ها و اولویت تعریف هر زیر پروژه کمک می‌کند.

به طور مثال خروجی برنامه‌ریز، برای چند نمونه از ادارات مختلف، از بین تمام ادارات یک سازمان بزرگ، در بخش ۷- ضمایم آمده است.

تولید این خروجی‌ها با همه کارآمدی و دانش گسترده‌ای که پشت آنهاست، چند ثانیه بیشتر طول نکشیده است.

به منظور ادامه این پژوهش می‌توان برخی از بخش‌های این برنامه‌ریز را بهبود بخشید و یا آن را با مدل‌ها و استانداردهای دیگر آزمود.

در نهایت، پیشنهاد می‌شود به‌جای استفاده از محدودیت عمومی‌در نظر گرفتن سطح بلوغ در انتخاب کاندیداها، با هوشمندی بیشتر، برخی اوقات برنامه‌ریز به دلایلی، از کنترل‌های سطوح بلوغ بالاتر نیز کنترل پیشنهاد کند، گرچه که همه کنترل‌های قبلی انتخاب نشده باشند. در جدول (۴)، مقایسه روش پیشنهاد شده با دیگر روش‌های مشابه آمده است.

جدول (۴) : مقایسه روش پیشنهادی با سایر الگوها

الگوریتم / معیار	روش سنتی انسانی	برنامه ریز پیشنهادی	دکسترا	ارسال-برچسب	ای-استار[1]	اچ‌تی‌ان[2]
هوشمندی	ندارد	دارد	ندارد	ندارد	دارد	ندارد
مبتنی بر جواب یا جمعیت	جواب	جمعیت	جمعیت	جمعیت	جمعیت	جمعیت
الهام از طبیعت	بله	بله	خیر	بله	خیر	بله
نیاز به حافظه	بله	خیر	بله	بله	بله	خیر
قطعیت	احتمالی	احتمالی	قطعی	قطعی	قطعی	قطعی
امکان افزودن پارامتر	خیر	بله	خیر	خیر	خیر	بله

ضمایم

در این بخش داده‌ها و نتایجی آمده است که می‌تواند در انواع سازمان‌ها که به صورت عمومی شامل این ادارات هستند، استفاده شود. در ادامه، ۴ نمونه از تنظیمات پیشنهادی ادارت که از لحاظ اهمیت دامنه‌های مدل بلوغ قابلیت امنیت سایبری تفاوت چشم‌گیرتری دارند و نتایج اجرای برنامه‌ریز روی هرکدام از تنظیمات، آمده است. در هر جدول ستون کد کنترل حاوی اندیسی است که مدل بلوغ قابلیت امنیت سایبری، یک کنترل را با آن اندیس می‌شناسد. این کد متشکل از مخفف انگلیسی دامنه طبق جدول (۱)، یک عدد و یک حرف الفبای انگلیسی بوده که تنها ترتیب آن کنترل در استاندارد را معرفی می‌کند.

۱- ادارات حراست:

جدول (۵): تنظیمات در نظر گرفته شده برای اداره حراست

درصد اهمیت	دامنه
۱۰۰	مدیریت دارایی، تغییر و پیکربندی
۵	مدیریت برنامه امنیت سایبری
۵۰	مدیریت روابط برون‌سازمانی و زنجیره تامین
۱۰۰	مدیریت دسترسی و هویت
۹۵	پاسخ به رویداد و رخداد، تداوم عملیات
۹۸	ارتباطات و به اشتراک گذاری اطلاعات
۹۰	مدیریت ریسک
۱۰۰	آگاهی از وضعیت
۳۰	مدیریت آسیب پذیری و تهدید
۱۰۰	مدیریت منابع انسانی

جدول (۶): بخشی از خروجی برنامه‌ریز با تنظیمات اداره حراست

عنوان	کد کنترل	سطح بلوغ	اولویت
دسترسی وقتی که دیگر مورد نیاز نیست باطل شود.	IAM-2c	۱	۱
فعالیت‌های آگاهی بخشی امنیت سایبری انجام شود.	WM-4a	۱	۲
مسئولیت‌های امنیت سایبری برای حوزه کاری شناسایی شوند.	WM-1a	۱	۳
کارکنانی جهت پاسخگویی به رویدادها و رخدادهای امنیت سایبری تعیین شده، شرح وظایف آن‌ها مشخص شود.	IR-3a	۱	۴
رویدادهای امنیت سایبری مهم و رخدادها ثبت و رهگیری شوند.	IR-2c	۱	۵
به رویدادهای مهم و رخدادهای امنیت سایبری به منظور کاهش تاثیر آن‌ها بر حوزه کاری و بازگرداندن به عملیات عادی، پاسخ داده شود.	IR-3b	۱	۶
رویدادهای امنیت سایبری برای تعیین اهمیت و اعلام رخدادهای امنیت سایبری تحلیل شوند.	IR-2b	۱	۷
یک نقطه تماس (شخص یا پست سازمانی) ایجاد شود که رویدادهای امنیت سایبری را می‌توان به او گزارش داد.	IR-1a	۱	۸
برنامه‌های تداوم برای حفظ و بازگرداندن عملیات حوزه کاری تدوین شود.	IR-4c	۱	۹
معیارهایی برای تعیین رویدادهای مهم امنیت سایبری شامل معیارهای اعلام رخدادهای امنیت سایبری ایجاد شود.	IR-2a	۱	۱۰

۲- ادارات بهداشت و سلامت:

جدول (۷): تنظیمات در نظر گرفته شده برای بهداشت

درصد اهمیت	دامنه
۱۰	مدیریت دارایی، تغییر و پیکربندی
۵	مدیریت برنامه امنیت سایبری
۲۰	مدیریت روابط برون‌سازمانی و زنجیره تامین
۸۰	مدیریت دسترسی و هویت
۱۰۰	پاسخ به رویداد و رخداد، تداوم عملیات
۹۵	ارتباطات و به اشتراک گذاری اطلاعات
۱۰۰	مدیریت ریسک
۷۰	آگاهی از وضعیت
۳۰	مدیریت آسیب پذیری و تهدید
۹۸	مدیریت منابع انسانی

جدول (۸): بخشی از خروجی برنامه‌ریز با تنظیمات بهداشت

عنوان	کد کنترل	سطح بلوغ	اولویت
رویدادهای امنیت سایبری برای تعیین اهمیت و اعلام رخدادهای امنیت سایبری تحلیل شوند.	IR-2b	۱	۱
کارکنانی جهت پاسخگویی به رویدادها و رخدادهای امنیت سایبری تعیین شده، شرح وظایف آن‌ها مشخص شود.	IR-3a	۱	۲
رویدادهای امنیت سایبری مهم و رخدادها ثبت و رهگیری شوند.	IR-2c	۱	۳
ریسک‌های امنیت سایبری شناسایی شوند.	RM-2a	۱	۴
معیارهایی برای تعیین رویدادهای مهم امنیت سایبری شامل معیارهای اعلام رخدادهای امنیت سایبری ایجاد شود.	IR-2a	۱	۵
برنامه‌های تداوم برای حفظ و بازگرداندن عملیات حوزه کاری تدوین شود.	IR-4c	۱	۶
یک نقطه تماس (شخص یا پست سازمانی) وجود داشته باشد که رویدادهای امنیت سایبری را می‌توان به او گزارش داد.	IR-1a	۱	۷
به رویدادهای مهم و رخدادهای امنیت سایبری به منظور کاهش تاثیر آن‌ها بر حوزه کاری و بازگرداندن به عملیات عادی، پاسخ داده شود.	IR-3b	۱	۸
ریسک‌های شناسایی شده پاسخ داده شود (اجتناب، کاهش، انتقال یا پذیرش).	RM-2b	۱	۹
مسئولیت‌های امنیت سایبری برای حوزه کاری شناسایی شوند.	WM-1a	۱	۱۰

۳- ادارات مالی و دارایی:

جدول (۹): تنظیمات در نظر گرفته شده برای اداره مالی و دارایی

درصد اهمیت	دامنه
۱۰۰	مدیریت دارایی، تغییر و پیکربندی
۵	مدیریت برنامه امنیت سایبری
۹۵	مدیریت روابط برون‌سازمانی و زنجیره تامین
۱۰۰	مدیریت دسترسی و هویت
۵۰	پاسخ به رویداد و رخداد، تداوم عملیات
۱۰	ارتباطات و به اشتراک گذاری اطلاعات
۶۰	مدیریت ریسک
۹۷	آگاهی از وضعیت
۱۰	مدیریت آسیب پذیری و تهدید
۹۴	مدیریت منابع انسانی

جدول (۱۰): بخشی از خروجی برنامه‌ریز با تنظیمات اداره مالی و دارایی

عنوان	کد کنترل	سطح بلوغ	اولویت
دسترسی وقتی که دیگر مورد نیاز نیست باطل شود.	IAM-2c	۱	۱
مسئولیت‌های امنیت سایبری برای حوزه کاری شناسایی شوند.	WM-1a	۱	۲
فعالیت‌های آگاهی بخشی امنیت سایبری انجام شود.	WM-4a	۱	۳
فهرستی از دارایی‌های اطلاعاتی که برای ارائه حوزه کاری مهم هستند، ایجاد شود. برای مثال: داده‌های مالی و اطلاعات کاربران.	ACM-1b	۱	۴
فهرستی از دارایی‌های IT و OT که جهت ارائه حوزه کاری مهم هستند، ایجاد شود.	ACM-1a	۱	۵
تغییرات مربوط به دارایی‌های فهرست شده قبل از پیاده‌سازی، ارزیابی شوند.	ACM-3a	۱	۶
محیط‌های عملیاتی رصد می شوند تا رفتارهای غیر عادی (نشانه یک رویداد امنیت سایبری محتمل) شناسایی شوند.	SA-2b	۱	۷
تامین کنندگان مهم IT و OT شناسایی شود (مثال: طرف‌های برون سازمانی که ارائه خدمات به آن‌ها بستگی دارد و شرکای کاری).	EDM-1a	۱	۸
الزامات امنیت سایبری حین برقراری رابطه با تامین‌کنندگان و دیگر طرف‌های ثالث در نظر گرفته شوند.	EDM-2b	۱	۹
مشتریان مهم شناسایی شوند (مثال: طرف‌های برون سازمانی که خدمات به آن‌ها ارائه شود).	EDM-1b	۱	۱۰

جدول (۱۲): بخشی از خروجی برنامه‌ریز با تنظیمات اداره انفورماتیک

عنوان	کد کنترل	سطح بلوغ	اولویت
دسترسی وقتی که دیگر مورد نیاز نیست باطل شود.	IAM-2c	۱	۱
کارکنانی جهت پاسخگویی به رویدادها و رخدادهای امنیت سایبری تعیین شده، شرح وظایف آن‌ها مشخص شود.	IR-3a	۱	۲
برنامه‌های تداوم برای حفظ و بازگرداندن عملیات حوزه کاری تدوین شود.	IR-4c	۱	۳
رویدادهای امنیت سایبری برای تعیین اهمیت و اعلام رخدادهای امنیت سایبری تحلیل شوند.	IR-2b	۱	۴
یک نقطه تماس (شخص یا پست سازمانی) وجود داشته باشد که رویدادهای امنیت سایبری را بتوان به او گزارش داد.	IR-1a	۱	۵
فعالیت‌های آگاهی بخشی امنیت سایبری انجام شود.	WM-4a	۱	۶
معیارهایی برای تعیین رویدادهای مهم امنیت سایبری شامل معیارهای اعلام رخدادهای امنیت سایبری ایجاد شود.	IR-2a	۱	۷
مسئولیت‌های امنیت سایبری برای حوزه کاری شناسایی شوند.	WM-1a	۱	۸
ریسک‌های امنیت سایبری شناسایی شوند.	RM-2a	۱	۹
رویدادهای امنیت سایبری مهم و رخدادها ثبت و رهگیری شوند.	IR-2c	۱	۱۰

۴- ادارات انفورماتیک:

جدول (۱۱): تنظیمات در نظر گرفته شده برای اداره انفورماتیک

درصد اهمیت	دامنه
۱۰۰	مدیریت دارایی، تغییر و پیکربندی
۹۵	مدیریت برنامه امنیت سایبری
۷۰	مدیریت روابط برون‌سازمانی و زنجیره تامین
۱۰۰	مدیریت دسترسی و هویت
۱۰۰	پاسخ به رویداد و رخداد، تداوم عملیات
۹۰	ارتباطات و به اشتراک گذاری اطلاعات
۱۰۰	مدیریت ریسک
۱۰۰	آگاهی از وضعیت
۹۸	مدیریت آسیب پذیری و تهدید
۱۰۰	مدیریت منابع انسانی

مراجع

[1] M. Boddy, J. Gohde, T. Haigh and S. Harp, "Course of action generation for cyber security using classical planning.," in ICAPS'05 Proceedings of the Fifteenth International Conference on International Conference on Automated Planning and Scheduling., 2005.

[2] L. Dubsky, "Assessing Security Controls: Keystone of the Risk Management Framework.," ISACA Journal, 2017.

[3] U. Faisst and O. Prokein, "An optimization model for the management of security risks in banking companies.," in IEEE, 2005.

[4] S. Goel, "Quantification, Optimization and Uncertainty Modeling in Information Security Risks: A Matrix-Based Approach.," Information Resources Management Journal (IRMJ), 2010.

[5] L. Hajjem, S. Benabdallah and F. Ben Abdelaziz, "A dynamic resource allocation decision model for IT security.," in IEEE, 2010.

[6] J. Milošević, H. Sandberg, K. H. Johansson and T. Tanaka, "Exploiting Submodularity in Security Measure Allocation for Industrial Control Systems.," in Proceedings of the 1st ACM Workshop on the Internet of Safe Things., 2017.

[7] J. Milošević, A. Teixeira, K. H. Johansson and T. Tanaka, "Security measure allocation for industrial control systems: Exploiting systematic search techniques and submodularity.," International Journal of Robust and Nonlinear Control, 2018.

[8] A. Razaque, C. Bach, N. salama and A. Alotaibi, "Fostering Project Scheduling and Controlling Risk Management.," in Department of Computer Science and Engineering University of Bridgeport, USA, 2012.

[9] س. پوررضا, "توسعه یک مدل فازی جهت تحلیل مخاطرات امنیتی در سیستم‌های اطلاعاتی سازمان‌ها (مورد کاوی: شرکت داروسازی بهستان تولید)," دانشگاه تربیت مدرس، دانشکده مهندسی, ۱۳۹۲.

[10] م. خاک بیز, "شناسایی و اولویت‌بندی عوامل موثر بر امنیت سیستم‌های اطلاعاتی سازمان با استفاده از مدل‌های تصمیم‌گیری چند شاخصه," دانشگاه یزد, ۱۳۹۵.

[11] پ. موسوی, "شناسایی و اولویت بندی ریسک‌های امنیت اطلاعات سازمانی بر اساس استانداردهای ایزو آی ای سی ۲۷۰۰۲ و کوبیت۴," دانشگاه تربیت معلم - تهران, ۱۳۹۳.

[12] The US. Department of Energy (DOE), "Cybersecurity Capability Maturity Model," 2014.

[13] شرکت فراکنش, "سامانه برنامه‌ریزی امنیت سازمانی یا Enterprise Security Planning (ESP) " تهران, ۱۳۹۷.

[14] M. Talaie, A. Mousavi and A.R. Sayadi, "Highest-Level Implementation of Push–Relabel Algorithm to Solve Ultimate Pit Limit Problem" in Journal of Mining and Environment (JME), 2020.

[15] The US. Department of Energy (DOE), "Cybersecurity Capability Maturity Model (C2M2) Program - C2M2 Model v2.0 Update – Invitation to Participate", 2021.