دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۳، جلد ۲۲، شماره ۱ (۷۴–۸۸)
https://monadi.isc.org.ir

روش تحلیل مخاطرات ماژول‌های زیرساخت ارتباطی و اطلاعاتی و استخراج الزامات پیشگیرانه امنیتی

نسرین تاج*، امیرمنصور یادگاری، ابوذر عربسرخی و رضا کلانتری
پژوهشگاه فناوری اطلاعات و ارتباطات، تهران، ایران

اطلاعات مقاله

تاریخچه مقاله:
تاریخ دریافت: ۱۸ اردیبهشت ۱۴۰۳
تاریخ پذیرش: ۴ مهر ۱۴۰۳
انتشار آنلاین: ۷ آبان ۱۴۰۳

کلمات کلیدی:
تهدیدات و آسیب‌پذیری ها
روش تحلیل مخاطره
منبع و نوع تهدید
الزامات امنیتی

نوع مقاله: پژوهشی

چکیده

با توجه به مصوبات شورای عالی فضای مجازی، توسعه زیرساخت کشور به عنوان زیرساختی مستقل، امن و پایدار یکی از اولویت‌های راهبردی کشور است که تحقق آن علاوه بر نیازمندی‌های فناورانه در زمینه فناوری اطلاعات و ارتباطات، بسترسازی برای استقرار و توسعه و عرضه انواع خدمات و محتوای فضای سایبری کشور؛ نیازمند تأمین ارتباطات امن و پایدار زیرساخت‌های حیاتی کشور نیز می‌باشد. براساس مدل مفهومی مندرج در مصوبه جلسه ۶۶ شورای عالی فضای مجازی، زیرساخت ارتباطی و اطلاعاتی کشور از یکسری ماژول‌های اصلی تشکیل شده است که تحلیل مخاطرات آن درراستای قابلیت بازگشت‌پذیری در حوادث، حفاظت‌شدگی در برابر تهدیدات، پایش و پاسخ هوشمند از نیازهای اساسی دستیابی به ارتباطات امن و مطمئن است. با توجه به محدودیت فضای این مقاله، نویسنده قصد دارد نحوه دستیابی به تحلیل مخاطرات براساس روش تلفیقی از کیفی، کمّی و نیمه کمی، چندنمونه از این ماژولهای اساسی را تشریح نموده و سپس بر اساس نتیجه بدست آمده، چگونگی بهره برداری از دانش پدیدآمده را در قالب نمودار جهت شناسایی نوع تهدید و منبع آن و استخراج الزامات امنیتی پیشگیرانه مذکور، تبیین نماید.

© ۱۴۰۳ انجمن رمز ایران

۱ مقدمه

بخش‌های زیادی از شبکه موجود در کشور به شدت وابسته به شبکه جهانی اینترنت است که مدیریت و حاکمیت این شبکه را در داخل کشور با مشکلاتی مواجه نموده است. این وابستگی نه تنها هزینه‌های زیادی را به کشور تحمیل می‌کند، بلکه از نظر پایداری و امنیت نیز غیرقابل اعتماد است. از این رو سیاست‌گذاری و اتخاذ رویکردهای مناسب برای چگونگی تأمین و تضمین ارتباطات و اطلاعات، به صورت امن و مطمئن در فضای مجازی کشور، اهمیت و ضرورت حیاتی دارد. در این راستا با توجه به مصوبات شورای عالی فضای مجازی، توسعه زیرساخت ارتباطی و اطلاعاتی مستقل، امن و پایدار یکی از اولویت‌های راهبردی کشور است. تحقق این امر نیازمند تأمین ارتباطات امن و پایدار زیرساخت‌های حیاتی کشور نیز می‌باشد که خود نیازمند تحلیل مخاطره ماژولهای زیرساختی در این حوزه است [۱].

جهت انجام این مهم ابتدا شناسایی و گردآوری استانداردها و چارچوب‌های مرتبط با حوزه هدف باید صورت گیرد. سپس شناسایی دارایی‌های اصلی این حوزه با ملاحظه اهمیت آنها از طریق استعلام از مالکان انجام پذیرد. در مرحله بعد استخراج تهدیدات و آسیب‌پذیری‌های هر ماژول در حوزه هدف از طریق ایجاد پرسشنامه، استناد به جلسات خبرگی و استفاده از استانداردهای جهانی این حوزه تبیین گردد. همچنین ارزش‌گذاری و کشف آسیب‌پذیری و تهدیدات مرتبط با آن، جهت ورود به فرایند تحلیل مخاطره الزامی است. از آنجایی که تحلیل مخاطره مورد نظر بر اساس حوزه مشخصی در این مقاله انجام گرفته است که بر اسناد بالادستی محرمانه تکیه دارد و طبق مصوبه ۶۶ فضای مجازی ماژول‌های

*نویسنده مسئول
آدرس‌های رایانامه: n_taj@itrc.ac.ir (نسرین تاج)، amyadegari@itrc.ac.ir (امیرمنصور یادگاری)، abouzar_arab@itrc.ac.ir (ابوذر عربسرخی)، kalantar@itrc.ac.ir (رضا کلانتری)
© ۱۴۰۳ تمامی حقوق متعلق به انجمن رمز ایران است.

اصلی زیرساخت ارتباطی و اطلاعاتی کاملاً مشخص شده‌اند لذا این تحلیل، دارایی محور بوده و دارایی‌ها همان ماژول‌های زیرساختی کشور در نظر گرفته شده‌اند.

در این بخش از مقاله ابتدا به بررسی و شناسایی استانداردهای مرتبط با این مهم پرداخته شده است و پس از توضیحات مختصر، نحوه استخراج تهدیدات و آسیب‌پذیری‌های مرتبط با دارایی‌های مفروض ذکر خواهد شد. پس از آن به تشریح روش تحلیل مخاطره پرداخته و در انتها نتیجه‌گیری مربوط به تحلیل دادگان، ارائه می‌گردد. این روش از آن جهت حائز اهمیت است که می‌تواند با دادگان متفاوت مانند ابزاری برای تحلیل مخاطرات مرتبط با موضوع عمل کند. همچنین یادآور می‌شود که نتایج اصلی ارائه شده در این مستند به دلیل اهمیت و حساس بودن موضوع، تا حدی شبیه‌سازی شده است.

بر اساس مجموعه موارد فوق، باید به این موضوع توجه داشت که پژوهش حاضر مبتنی بر روش آمیخته مشتمل بر مطالعات کیفی (جهت مطالعه نظام‌مند اسناد فرادست، استانداردهای امنیتی مرتبط و تحلیل تهدیدات و مخاطرات امنیتی مربوطه) و نیز مطالعات کمّی (جهت شناسایی و تحلیل مخاطرات و اولویت‌گذاری آنها مبتنی بر نظرات نخبگان و کارشناسان این حوزه) بنا نهاده شده است. بنابراین کلیه نتایج و دستاوردهای حاصله مبتنی بر قلمرو مطالعاتی فوق ارائه گردیده است و در این مرحله ارزیابی کمّی و میدانی ماژول‌های زیرساخت ارتباطی و اطلاعاتی لحاظ نگردیده است.

۲ شناسایی و استخراج مستندات داخلی و خارجی

مستندات خارجی مرتبط با این پروژه شامل استانداردهای مورد استفاده برای بحث تحلیل مخاطرات است. همچنین منظور از اسناد داخلی همان اسناد بالادستی است که به اهمیت شبکه زیرساختی کشور و ملزومات و ماژول‌های تشکیل دهنده آن پرداخته است. در ادامه این مقاله ضمن بررسی استانداردهای مرتبط، در تبیین محتوای لازم از اسناد بالادستی این حوزه بهره‌برداری خواهد شد.

۱.۲ استانداردها و آیین‌نامه‌ها

از آنجا که در این مستند، محوریت با تحلیل مخاطرات مربوط به اجزای اصلی زیرساخت و استخراج الزامات است، نیاز به الگوبرداری و تعیین استانداردهایی در همین حوزه خواهد بود. در بین استانداردهای پیشنهادی، استانداردهایی چون NIST800-30 و ISO/IEC 27005 و ISO/IEC 27014 و NIST CSF جهت انجام تحلیل مخاطره، به طور مفصل مورد بررسی قرار گرفته‌اند که در ادامه به اختصار به بررسی اهم این استانداردها خواهیم پرداخت.

لازم به ذکراست که ISO/IEC 27014 راهنمایی لازم در مورد اصول و فرآیندهای حاکمیت امنیت اطلاعات را فراهم می‌کند و توسط آن سازمان می‌تواند مدیریت امنیت اطلاعات را ارزیابی، هدایت و نظارت نماید که البته بحث نظارت و ارزیابی، در محوریت این مقاله نیست.

۱.۱.۲ استاندارد NIST CSF

چارچوب امنیت سایبری NIST برای پاسخ به دستورالعمل اجرایی ۱۳۶۳۶ ریاست جمهوری وقت آمریکا ارائه شد. هدف اصلی این دستورالعمل، ارتقا امنیت زیرساخت‌های حیاتی کشور در برابر حملات داخلی و خارجی است. با وجود این، بسیاری از سازمان‌های خصوصی نیز از این چارچوب برای تقویت دفاع سایبری خود استفاده می‌کنند. به طور خاص، NIST CSF پنج عملکرد اصلی را برای مدیریت ریسک‌های موجود در امنیت داده‌ها و اطلاعات توصیه می‌کند. این عملکردها عبارتند از: شناسایی، محافظت، تشخیص، پاسخ‌گویی و بازیابی [۲].

۲.۱.۲ استاندارد ISO 27005

هدف از تدوین استاندارد ISO/IEC 27005، تعیین راهنمایی برای مدیریت مخاطرات امنیت اطلاعات است.این استاندارد مفاهیم کلی مشخص شده در استاندارد ISO/IEC 27001 را پوشش می‌دهد و برای کمک به پیاده‌سازی مطلوب امنیت اطلاعات، براساس رویکرد مدیریت مخاطرات طراحی شده است. مدیریت مخاطرات امنیت اطلاعات، شامل مراحل زمینه‌سازی، شناسایی مخاطره، تحلیل مخاطره، ارزیابی مخاطره، مقابله با مخاطره، پذیرش مخاطره، تبادل اطلاعات و رایزنی مخاطره، پایش و بازنگری مخاطره می باشد. این استاندارد چارچوب کاری مدیریت مخاطرات امنیت اطلاعات مبتنی بر مجموعه استانداردهای 27k و مدل عمومی ISO27001 معرفی می‌کند.همچنین چارچوب مدیریت مخاطرات معرفی شده در ISO27005 قابل بکارگیری در همه انواع سازمان‌ها (به عنوان مثال شرکت‌های تجاری، نهادهای دولتی، سازمان‌های غیرانتفاعی) است که مایلند مخاطرات امنیت اطلاعات سازمان خود را کاهش دهند [۴].

۳.۱.۲ استاندارد NIST800-30

این استاندارد به عنوان راهنمای اجرای تحلیل مخاطره برای سامانه‌ها و دارایی‌های اطلاعاتی و به عنوان روش اجرایی و راهنمای تکمیلی چارچوب NIST 800-39 شناخته می‌شود. هدف نهایی NIST 800-30 کمک به سازمان‌ها در بهبود مدیریت مخاطرات فناوری اطلاعات و ایجاد سه محور کارکردی شامل تحلیل مخاطره، برخورد مخاطره و پایش مخاطره است.

به طور کلی NIST 800-30 یک شیوه سناریو محور در تحلیل مخاطره ارائه می‌دهد و قابلیت برآورد کمّی و کیفی مخاطره را دارد. این مدل شامل فهرستی از تهدیدات و آسیب‌پذیری‌های رایج می‌باشد. ضمایم H، F و D دسته‌بندی و فهرستی از دارایی‌ها، آسیب‌پذیری‌ها و تهدیدات رایج را برای انجام فرآیند تحلیل مخاطرات آورده است [۶].

۲.۲ نگاشت استانداردهای امنیتی با نیازمندی‌های زیرساخت ارتباطی و اطلاعاتی کشور

در مطالعات مربوطه [۹] مدل های رایج جهت ایجاد برنامه جامع امنیت و شیوه های ارزیابی مخاطرات امنیت سایبری زیرساخت ارتباطی و اطلاعاتی کشور مورد بررسی و مطالعه قرار گرفتند. نتیجه آنکه با توجه به نیازمندی این زیرساخت در دو بخش ارتباطی و اطلاعاتی هر یک از مدل‌های امنیتی و چارچوب‌های کاری NIST CSF و ISO27001/ISMS قابل استفاده می‌باشند. این مدل های امنیتی در پاسخ به نیازمندی‌های کلان زیرساخت کشور در تعیین راهبرد و مدل حاکمیت امنیت و مدیریت مخاطرات زیرساخت ارتباطی و اطلاعاتی پیشنهاد شده‌اند و قابل نگاشت به قلمرو زیرساخت امنیتی کشور می باشند. چارچوب های کاری و مدل‌های امنیتی با ارائه محورهای اقدام طرح امنیت و شیوه سنجش اثربخشی اقدامات، به شناسایی قابلیت‌های امنیتی زیرساخت ارتباطی و اطلاعاتی کشور کمک می‌کنند.

در بخش شیوه‌های مدیریت و ارزیابی مخاطرات، روش‌های مورد نیاز و قابل کاربرد در فرآیندی تحلیل مخاطره مرتبط با اجزا و دارایی‌های زیرساخت ارتباطی و اطلاعاتی بررسی و مورد سنجش قرار گرفتند و در نهایت دو شیوه منتخب ISO27005 و NIST 800-30 به منظور تطابق با مدل‌های امنیتی پیشنهادی، ارائه شد.

۳ شناسایی دارایی‌ها، تهدیدات وآسیب‌پذیری‌های زیرساخت ارتباطی و اطلاعاتی کشور

زیرساخت امنیتی کشور، بنابر مصوبات شورای عالی فضای مجازی، زیرساخت ارتباطی و اطلاعاتی فضای سایبری است. این شبکه علاوه بر بسترسازی برای استقرار، توسعه و عرضه انواع خدمات و محتوای فضای سایبری کشور، مأموریت تأمین ارتباطات امن و پایدار زیرساخت‌های حیاتی کشور را بر عهده داشته و از این منظر، مهم‌ترین سرمایه ملی سایبری کشور است. با این وجود شواهد نشان می‌دهد که این شبکه در امنیت سایبری همچنان با خلأ روبرو است و تبادل داده در فضای مجازی کشور تضمین شده نیست و سیاستگذاری، طراحی، توسعه و ارتقای امنیت سایبری و مصون‌سازی در این شبکه، در مقابل بردارهای مختلف تهدید باید به طور گسترده مورد توجه قرار گیرد. لذا شناخت دارایی‌ها و تهدیدات مرتبط با دارائی‌ها و الزامات امن‌سازی در درجه نخست اهمیت است. بر اساس مدل مفهومی مندرج در مصوبه جلسه ۶۶ شورای عالی فضای مجازی، زیرساخت امنیتی کشور از دو بخش زیرساخت (ارتباطی و اطلاعاتی) و خدمات تشکیل شده است. در شکل ۱ اجزای زیرساخت امنیتی کشور به تصویر کشیده شده است.

از طرفی به منظور تشخیص و اولویت‌بندی تهدیدها و آسیب‌پذیری‌ها در سطح شبکه، ارزیابی و تحلیل مخاطرات به صورت فرآیندی و بر مبنای تهدیدات این شبکه مورد نیاز است. لازم به ذکر است که جهت شناسایی بهتر نقاط ضعف لایه‌های زیرساختی شبکه، برخی از تهدیدات و آسیب‌پذیری‌های لایه‌های زیرساخت‌های ارتباطی و اطلاعاتی شبکه بر اساس مطالعات تطبیقی انجام شده است.

در ادامه به منظور تحلیل مخاطره و ارزیابی امنیتی ماژول های زیرساختی شبکه در این بخش به تعریف مفاهیم مرتبط با مخاطره خواهیم پرداخت.

۱.۳ آسیب‌پذیری

آسیب‌پذیری را می‌توان میزان قابلیت بهره‌گیری از یک نقطه ضعف دانست، که با توجه به دارایی‌ها مشخص می‌گردند. همچنین آسیب‌پذیری‌های موجود در هر سیستمی را می‌توان در شش گروه طبقه‌بندی نمود [۵]:

- فیزیکی (مانند تمهیدات امنیتی فیزیکی ضعیف در برابر دسترسی غیرمجاز)
- طبیعی (مانند قرار گرفتن بر روی گسل زلزله)
- سخت‌افزار (مانند طراحی و تولید نامناسب از لحاظ بدنه و اجزا)
- نرم‌افزار (مانند ضعف در کدنویسی، مشکلات برنامه‌نویسی)
- رسانه (مانند سبک و قابل حمل بودن)
- ارتباطات (مانند فقدان تمهیدات امنیتی مناسب)
- فردی (مانند عدم توانایی در شناسایی و تشخیص)

۲.۳ تهدید

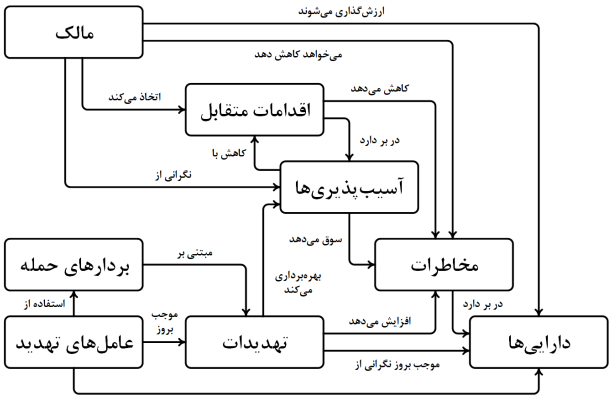
تهدید عامل اصلی بروز مخاطره و ایجاد لطمه یا خسارت به دارایی‌های اطلاعاتی می‌باشد که با استفاده از آسیب‌پذیری موجود موجب بروز مخاطره می‌گردد. شکل ۲ رابطه بین آسیب‌پذیری، دارایی و تهدید را نشان می‌دهد. تهدید و عامل تهدید یکی از مهمترین عوامل مورد بررسی در بحث ارزیابی مخاطره هستند. یك تهدید عبارت از یك رویداد با اثر نامطلوب می‌باشد که باعث ایجاد لطمه به دارایی‌های اطلاعاتی است [۵]. به عبارتی تهدید با استفاده از آسیب‌پذیری موجود موجب بروز مخاطراتی می‌گردد که باعث لطمه یا از دست رفتن دارایی است. اثر عامل تهدید برروی تهدیدات یك عامل ایجادی است و بر روی دارایی‌ها، یك عامل ایجابی است که مالك دارایی می‌تواند ضمن آگاهی از آن با اقدامات متقابل تأثیر آن را بروی دارایی‌های ارزشمند مهار نماید.

۳.۳ نتایج حاصل از وقوع تهدید و آسیب‌پذیری

برای مخاطره تعاریف مختلفی وجود دارد اما در اصل هدف نهایی آنها یك چیز می‌باشد. مخاطره زمانی اتفاق می‌افتد که یك تهدید شناخته‌شده یا ناشناخته، از آسیب‌پذیری موجود استفاده نموده و از طریق آن به دارایی‌های یك شخص یا سازمان آسیب وارد نماید. دارایی‌ها ممکن است ملموس یا غیرملموس باشند [۴]. به عبارتی می‌توان مخاطره را حاصل از پیوند بین تهدید و آسیب‌پذیری دانست.

به فرآیند شناسایی دارایی‌ها و ارزش آن‌ها، تعیین آسیب‌پذیری‌ها،

شکل ۱. اجزای زیرساخت ارتباطی و اطلاعاتی کشور [۳]



شکل ۲. رابطه بین آسیب‌پذیری،دارایی و تهدید [۵]

چگونگی احتمال سوءاستفاده از آن‌ها، تهدیدات و احتمال وقوع آن‌ها و در نهایت ارزش‌گذاری مخاطره، ارزیابی مخاطره گفته می‌شود [۷] با ارزیابی مخاطره یك سازمان می‌تواند تأثیر کنترل‌های امنیتی فعلی و میزان حفاظت از دارایی‌های خود را بسنجد.

۴ مدل و روش تحلیل مخاطرات زیرساخت ارتباطی و اطلاعاتی کشور

در بررسی امن‌سازی زیرساخت کشور، تحلیل مخاطرات مرتبط با زیرساخت‌های اطلاعاتی و ارتباطی نقش کلیدی ایفا می‌نماید، لذا انتخاب مدل و تشریح متدولوژی تحلیل مخاطره، مراحل انجام تحلیل و معیار پذیرش مخاطرات از جمله مباحث اصلی است که در این بخش به آن‌ها پرداخته می‌شود. درخصوص انتخاب روش تحلیل در این مستند با توجه به شاخص های طرح شده در گزارش بررسی و انتخاب متدولوژی تحلیل مخاطرات کشور [۱۰] از میان ۱۸ روش مورد بررسی برای تحلیل مخاطره زیرساخت کشور، دو متدلوژی ISO 27005 و NIST 800-30 به عنوان روش‌های برتر برگزیده شده‌اند. برخی از مهم‌ترین مزایای استفاده از دو متد فوق عبارتند از:

- فراوانی استفاده و تعداد زیاد کاربران
- دسترس پذیری اسناد و مراجع
- قابلیت پشتیبانی از هر دو رویکرد تحلیل سناریو محور و دارایی محور
- قابلیت پشتیبانی از دو رویکرد کمّی و کیفی در محاسبه مخاطره
- قابلیت سازگاری و تعامل‌پذیری با دیگر روش‌ها و استانداردهای امنیتی

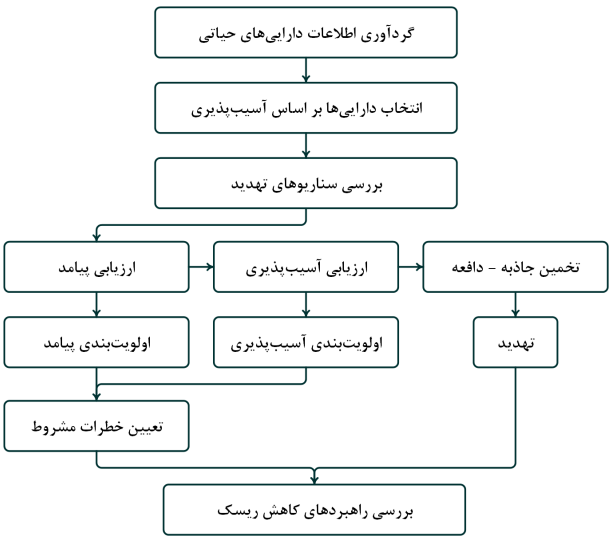
درخصوص انتخاب مدل تحلیل مخاطرات زیرساخت امنیتی کشور با توجه به معیارهای اساسی تأثیرگذار، مدل مناسبی برای ارتباط بین اجزای تحلیل مخاطره در نظر گرفته شده است [۸]. این معیارها شامل موارد ذیل است:

- دارایی‌ها
- تهدیدات
- آسیب‌پذیری‌ها
- پیامد ناشی از تهدید که در واقع همان اثر مخاطره بر روی مؤلفه‌های سه‌گانه امنیت (CIA) است.

۱.۴ بیان رویکرد و روش اجرای تحلیل مخاطرات

به طور کلی پارامترهای درگیر در محاسبه مخاطره به سه شیوه کیفی، کمّی و نیمه کمّی قابل محاسبه هستند. دراین مستند برای اولین بار تحلیل مخاطره زیرساخت کشور از تلفیق هر سه روش استفاده شده است. بر این اساس بیش از ده‌ها سناریوی تهدید براساس نظرات خبرگی در این حوزه طراحی گردید که همزمان با ارزش‌گذاری دارایی توسط خبرگان تلفیق شد که در نهایت با بهره‌گیری از این دادگان کمّی و کیفی، نتایج و نمودارهای خوبی حاصل گردید.

در رویکرد تحلیل مخاطره، دو شیوه اصلی تهدید محور (سناریومحور) و دارایی محور (ضربه محور) وجود دارد. رویکرد تحلیل، در واقع جهت‌گیری شروع عملیات تحلیل مخاطره را مشخص می‌کند. در رویکرد تهدیدمحور بر استخراج سناریوهای تهدید و شناخت آسیب‌پذیری‌های مرتبط با آن‌ها



شکل ۳. مدل و ارتباط بین اجزای تحلیل مخاطره [۵]

تمرکز می‌شود. در حالی که در رویکرد دارایی محور تمرکز اصلی بر شناخت دارایی‌ها، ارزش و پیامد ناشی از وقوع تهدید است.

در تحلیل مخاطره زیرساخت کشور هر دو رویکرد فوق مورد استفاده قرار گرفته است. ابتدا با یک رویکرد دارایی محور، دارایی‌های اطلاعاتی و مؤلفه های زیرساخت امنیتی کشور شناسایی و ارزشگذاری شده است سپس با توسعه سناریوهای تهدید و آسیب‌پذیری‌های مرتبط با هر یک تحلیل مخاطره متناظر با هر دارایی انجام شده است. بکارگیری هر دو روش تهدید محور و دارایی محور موجب همپوشانی و جامعیت بهتر در پرداختن به مخاطرات در قلمرو کاری مورد بررسی می‌شود. در ادامه مراحل اجرای تحلیل و شیوه محاسبه مخاطره به تفصیل تشریح می‌گردد.

مراحل ارزیابی مخاطرات در زیرساخت ارتباطی و اطلاعاتی کشور شامل گام‌های شناسایی و ارزشگذاری دارایی‌ها، شناسایی و ارزشگذاری آسیب‌پذیری‌ها، شناسایی تهدید و تعیین احتمال وقوع تهدیدات، محاسبه اثر مخاطره بر المان‌های امنیتی و محاسبه مخاطره می‌باشد.

۲.۴ شناسایی و ارزشگذاری دارایی‌ها

هریک از دارایی‌های اطلاعاتی می‌بایست باتوجه سه مؤلفه اصلی امنیت، یعنی در دسترس بودن، محرمانگی و صحت، ارزش‌دهی شوند. این مؤلفه ها سه سطح مختلف، زیاد، متوسط و کم را به خود اختصاص می‌دهند که پارامترهای آن‌ها برای ارزشگذاری به شرح ذیل می‌باشد:

- در دسترس بودن
  - تأثیر ایجاد وقفه بر اعتبار سازمان
  - تأثیر وقفه دارایی بر خدمات دیگر
  - محدوده بهره‌برداران
  - وضعیت جایگزینی دارایی‌های اطلاعاتی
- محرمانگی
  - تأثیر افشای اطلاعات بر اعتبار سازمان
  - محدوده دسترسی افراد مجاز به اطلاعات
  - تأثیر افشای اطلاعات بر خدمات دیگر
- صحت
  - تأثیر دستکاری اطلاعات بر اعتبار سازمان
  - وضعیت جایگزین و پشتیبان اطلاعات
  - تأثیر دستکاری اطلاعات بر خدمات دیگر

پس از استعلام از مالکان دارایی، جدول ارزشگذاری دارایی بر اساس جدول ۱ تعیین شده است.

۳.۴ شناسایی و ارزشگذاری آسیب‌پذیری‌ها

یکی از مهمترین بخش‌های تحلیل مخاطره، پس از مرحله شناسایی و ارزشگذاری دارایی‌ها، شناسایی و ارزشگذاری نقاط ضعف و آسیب‌پذیری‌ها می‌باشد. برای این کار می‌توان از فهرست آسیب‌پذیری‌ها و تهدیدات اولیه دسته‌های دارایی که وجود دارد نیز استفاده نمود. دیگر ضعف‌های امنیتی نیز که ممکن است توسط یک مبدأ تهدید مورد استفاده قرار گرفته و سپس منجر به ضربه به دارایی‌ها و مختل نمودن فعالیت دارایی اطلاعاتی مربوطه گردد، باید شناسایی شوند.

هر یک از آسیب‌پذیری‌های شناخته شده، سه سطح مختلف کم، متوسط و زیاد را به خود اختصاص می‌دهند. همچنین در مواردی که آسیب‌پذیری مورد نظر برای دارایی کارایی نداشته باشد از کلمه کاربردناپذیر استفاده می‌شود. به منظور گسسته‌سازی این سطوح در مراحل بعدی کار، به ترتیب مقادیر ۰ تا ۳ برای کاربردناپذیر، کم، متوسط و زیاد در نظر گرفته شده است. به طور کلی می‌توان به دلیل کاربردپذیر نبودن آسیب‌پذیری در مورد یک دارایی از مطرح کردن آن خودداری نمود ولی برای روشن بودن فرآیند و مقایسه بهتر میان دارایی‌های موجود در یک دسته، در فرآیند ارزیابی مخاطرات، تمامی آسیب‌پذیری‌های فرآیندی–مدیریتی و فیزیکی مربوط به یک دسته برای دارایی قرار گرفته در آن دسته آورده شده و آسیب‌پذیری‌های کاربردناپذیر برای آن دارایی خاص، عدد صفر یا همان کاربردناپذیر را به خود اختصاص می‌دهند.

دلایل اینکه یك آسیب‌پذیری در چه سطحی قرار بگیرد در جدولی است که بر اساس استانداردهای این حوزه تهیه شده در پرسشنامه‌ها یا جلسات خبرگی در اختیار خبره و متخصصین این حوزه قرار می‌گیرد و براین مبنا ارزشگذاری آسیب‌پذیری انجام میشود.توضیحات بیشتر در خصوص این بخش در سند [۹] گردآوری شده است.

۴.۴ شناسایی و تعیین احتمال وقوع تهدیدات

مبتنی بر پژوهش‌های انجام شده از منابع معتبر نظیر سری NIST 800، ENISA، ISO 27k و پروژه‌های انجام شده پیشین در حوزه امنیت زیرساخت کشور، میتوان تهدیدات امنیتی را براساس نوع و منبع/منشأ بوجود آورده تهدید دسته بندی نمود.

جدول ۱. ارزش‌گذاری دارایی‌های زیرساخت ارتباطی و اطلاعاتی

ردیف	نام دارایی	دسته	محل استقرار	ارزش نهایی دارایی اطلاعاتی		
				در دسترس بودن (A)	صحت (B)	محرمانگی (C)
۱	شبکه هسته	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۳	۳	۳
۲	شبکه تجمیع	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۲	۲	۳
۳	شبکه دسترسی	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۲	۲	۲
۴	شبکه دولت	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۲	۲	۲
۵	شبکه‌های توزیع محتوا (CDN)	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۳	۳	۲
۶	خدمات نام دامنه (DNS)	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۳	۳	۳
۷	شبکه‌های اختصاصی	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۱	۲	۱
۸	شبکه (IXP)	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۳	۲	۳
۹	خدمات زمان شبکه (NTP)	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۳	۲	۲
۱۰	مراکز آزاد ICT	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۱	۲	۱
۱۱	گذرگاه ایمن داخلی	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۲	۲	۲
۱۲	گذرگاه ایمن مرزی	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۳	۳	۲
۱۳	قطب‌های مراکز داده	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۳	۳	۳
۱۴	مراکز داده اختصاصی	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۱	۲	۱
۱۵	مراکز داده عمومی	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۲	۲	۳
۱۶	مراکز رصد و پایش شبکه ملی اطلاعات	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۲	۳	۳
۱۷	مراکز تبادل پیام و اطلاعات	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۱	۲	۱
۱۸	زیرساخت ابری (عمومی، خصوصی و جهانی)	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۳	۳	۳
۱۹	مرکز مدیریت امنیت	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۳	۳	۳
۲۰	مراکز مدیریت سالم‌سازی	زیرساخت ارتباطی	زیرساخت شبکه ملی اطلاعات	۲	۲	۲

۵.۴ تعیین احتمال وقوع تهدید و شدت اثر مخاطره

در این مرحله اثر مخاطره بر روی المان‌های امنیتی شناسایی خواهد شد. از تلفیق هر زوج آسیب‌پذیری و تهدید مرتبط با آن، یک سناریوی مخاطره ایجاد خواهد شد که باید دید این مخاطره بر روی هر یک از سه المان امنیتی یعنی محرمانگی، صحت و در دسترس بودن اثر خواهد داشت یا خیر. این امر با توجه به ماهیت آسیب‌پذیری و تهدید مشخص خواهد شد. به عنوان مثال، تهدیدی به عنوان زلزله تنها بر روی در دسترس بودن دارایی اطلاعاتی، اثرگذار خواهد بود. اما تهدیدی همچون سرقت هم بر روی در دسترس بودن و هم بر روی محرمانگی اثر گذار خواهد بود.

با توجه به اینکه میزان مخاطرات پیش رو در ارتباط مستقیم با ارزش دارایی‌های اطلاعاتی و همچنین اثر مخاطرات بر روی المان‌های امنیتی می‌باشد، نیازمند مکانیزمی است تا به نوعی این عوامل در محاسبه مخاطرات دارایی‌های اطلاعاتی لحاظ گردند. بدین منظور با توجه به دو المان ارزش دارایی اطلاعاتی (در سه بعد امنیت اطلاعات) و همچنین اثر هر مخاطره بر روی المان‌های امنیت اطلاعات، ضربه به صورت (۱) محاسبه می‌گردد.

$$\text{Loss} = (I_c * C) + (I_i * I) + (I_a * A) \quad (۱)$$

در این مرحله، مخاطره دارائی اطلاعاتی با توجه به ورودی‌های تعیین شده و توسط رابطه‌های (۲) و (؟؟) محاسبه مخاطره صورت می‌پذیرد.

$$\text{Risk} = \text{Vulnerability} * \text{Threat} * \text{Loss} \quad (۲)$$

$$\text{Risk} = \text{Vulnerability} * \text{Threat} * (I_c * C) + (I_i * I) + (I_a * A) \quad (۳)$$

پس از اینکه برای هر زوج آسیب‌پذیری و تهدید مرتبط با یک دارایی اطلاعاتی، رابطه (؟؟) اعمال گردید، مجموع مخاطرات محاسبه شده، احتمال وقوع تهدید یا مخاطره نهایی دارایی را نشان می‌دهد.

$$\text{Risk Total Asset} = \sum \text{Risk} \quad (۴)$$

جدول ۲. تهدیدات امنیتی بر اساس نوع و منبع تهدید

ردیف	منبع/منشأ تهدید	شرح
۱	مهاجم متخاصم	افراد یا سازمان‌هایی هستند که قصد نفوذ به سیستم‌ها، به دست آوردن داده‌ها یا ایجاد تهدید امنیتی را در برابر یک سازمان یا شبکه دارند.
۲	تأمین‌کننده تجهیز و سرویس	فرد یا شرکتی است که به منظور تأمین تجهیزات و خدمات مورد نیاز یک سازمان یا شرکت مورد استفاده قرار می‌گیرد.
۳	راهبر با دسترسی ویژه	فردی است که دسترسی اختصاصی و بالا به یک سیستم یا شبکه را دراست و می‌تواند به منابع حاس، محدود و محرمانه دسترسی داشته باشد و تغییرات و تنظیمات اساسی آن را انجام دهد.
۴	جاسوس	فردی است که به صورت مخفیانه برای جمع آوری اطلاعات محرمانه عمل می‌کند.
۵	حوادث طبیعی	از دست رفتن یا خرابی سیستم‌ها و نرم‌افزارها به دلیل وقوع حوادث طبیعی مانند زلزله، سیل، آتش سوزی و ... اشاره می‌کند.

جدول ۳. معیار پذیرش مخاطرات

	ماتریس مقابله با مخاطرات									
	آسیب پذیری	۱			۲			۳		
	احتمال وقوع تهدید	۱	۲	۳	۱	۲	۳	۱	۲	۳
ضربه	جزئی ۰	A Accept	B Accept	C Accept	D Accept	E Accept	F Accept	G Accept	H Mitigate	I Mitigate
	جزئی ۲	J Accept	K Accept	L Accept	M Accept	N Accept	O Mitigate	P Accept	Q Mitigate	R Mitigate
	قابل ۳	S Accept	T Accept	U Accept	V Accept	W Mitigate	X Mitigate	Y Mitigate	Z Mitigate	@ Mitigate
	قابل ۵									
	بحرانی ۶									
	بحرانی ۹									

۶.۴ معیار پذیرش مخاطرات

برای تعیین سطح پذیرش مخاطرات از سه پارامتر «ارزش آسیب‌پذیری» و «احتمال وقوع تهدید» و «ضربه» استفاده خواهد شد. مطابق با آنچه که در بندهای «شناسایی و ارزش‌گذاری آسیب‌پذیری‌ها» و «شناسایی و تعیین احتمال وقوع تهدیدات»، برای تعیین سطوح آسیب‌پذیری‌ها و تهدیدات ارائه شده است، به هر یک از این سطوح، عددی (از صفر تا سه) اختصاص می‌یابد؛ همچنین با توجه به ارزش دارایی و اثر بر روی المان‌های امنیتی، ضربه محاسبه می‌شود. در مرحله کاهش مخاطرات، برای مقابله با مخاطرات غیر قابل پذیرش، راهکارهای مناسب ارائه خواهند شد. جدول ۳ معیار پذیرش مخاطرات را با توجه به سه المان معرفی شده، نشان می‌دهد. قالب اصلی این جدول براساس الگوی معرفی شده در استاندارد ISO/IEC 27005 می باشد، اما اعداد حاصله که منجر به تعیین نواحی از نظر کاهش یا پذیرش ریسک شده است در هر شبکه‌ای از لحاظ اهمیت و موقعیت متفاوت است. در این مستند بر اساس تحقیقات انجام شده بر مبنای پرسشنامه و نظرات خبرگی به انجام رسیده است.

معیار پذیرش مخاطرات، آن دسته از زوج آسیب‌پذیری‌ها و تهدیداتی است که مطابق با جدول ۳ در ناحیه سبز رنگ قرار می‌گیرند.مخاطراتی که در ناحیه‌های H، I، O، Q، R، W، X، Y، Z و @ قرار می‌گیرند، قابل پذیرش نمی‌باشند. لازم به ذکر است که با توجه به معیار پذیرش مخاطرات در جدول ۳، موارد زیر قابل استنتاج می‌باشد:

- آن دسته از مخاطراتی که دارای سطح آسیب‌پذیری کم می‌باشند، قابل پذیرش می‌باشند. زیرا اساساً با توجه به سطح آسیب‌پذیری، مخاطره ناشی از آن قابل پذیرش می‌باشد.
- آن دسته از مخاطراتی که دارای احتمال وقوع تهدید کم می‌باشند، قابل پذیرش می‌باشند. به جز در مواردی که سطح آسیب‌پذیری زیاد بوده و با توجه به ارزش دارایی، مخاطره دارای اثر زیاد بر روی المان‌های امنیتی باشد.
- آن دسته از مخاطراتی که دارای سطح آسیب‌پذیری متوسط و احتمال وقوع تهدید متوسط باشند، در صورتی که با توجه به ارزش دارایی، مخاطره دارای اثری زیاد بر المان‌های امنیتی نباشد، قابل پذیرش می‌باشد.
- آن دسته از مخاطراتی که دارای سطح آسیب‌پذیری متوسط و احتمال وقوع تهدید زیاد می‌باشند، اما با توجه به ضربه وارده، دارای اثری کم بر المان‌های امنیتی باشد، نیز قابل پذیرش می‌باشد. زیرا مخاطره حتی در صورت وقوع دارای اثری کم می‌باشد.

۵ تحلیل مخاطرات زیرساخت ارتباطی و اطلاعاتی

در این بخش، به تحلیل مخاطرات امنیتی برخی از دارایی‌های زیرساخت ارتباطی و اطلاعاتی پرداخته می‌شود. در ابتدا به ازای هر دارایی، به صورت خلاصه به چیستی آن دارایی اشاره می‌گردد، سپس به ارزیابی مخاطره دارایی مربوطه پرداخته می‌شود. در ارزیابی مخاطره، به مواردی چون فهرست تهدیدات، منبع تهدید، نوع تهدید، احتمال وقوع، آسیب‌پذیری مرتبط با تهدیدات، ارزش آسیب‌پذیری، اثر بر روی در دسترس بودن، اثر بر روی محرمانگی، اثر بر روی صحت، ضربه، مخاطره و استراتژی برخورد اشاره می‌گردد. در نهایت تحلیل مدیریتی در خصوص دارایی مربوطه ارائه می‌شود.

در این بخش با توجه به اینکه زیرساخت ارتباطی و اطلاعاتی کشور از ۲۰ ماژول اصلی تشکیل شده است، به صورت موردی برخی از دارایی‌های زیرساختی کشور مورد بررسی قرار می گیرد. لذا در ادامه تحلیل مخاطرات مربوط به ماژول هسته به عنوان ستون فقرات اصلی زیرساخت ارتباطی و ماژول ابر به عنوان جزء مهمی از زیرساخت اطلاعاتی معرفی خواهند شد.

۱.۵ تحلیل مخاطرات شبکه هسته

به منظور تحلیل مخاطرات ماژول هسته نیازبه شناخت این شبکه است. به همین منظور در ابتدا مروری به وضعیت شبکه هسته خواهیم داشت و در ادامه به تحلیل مخاطرات این شبکه خواهیم پرداخت.

۱.۱.۵ شناخت شبکه هسته

شبکه فوق‌سریع و پرظرفیتی است که امکان ارتباط میان شبکه‌های تجمیع و شبکه‌های خارجی (از جمله اینترنت) را فراهم می‌کند. این شبکه متناسب با نیازها و ملاحظات مندرج در اسناد بالادستی توسعه یافته و امکان تعامل مدیریت شده با سایر شبکه‌ها از جمله اینترنت را فراهم می‌آورد.

شبکه هسته یا شبکه اصلی داخلی، فقط از طریق گذرگاه‌های امن با شبکه‌های خارجی در ارتباط است. زیرشبکه‌های داخلی دیگر به این شبکه هسته متصل هستند و از طریق آن با یکدیگر ارتباط برقرار می‌کنند. برای این منظور، این شبکه باید بتواند ارتباطات داخلی را تامین نماید [۴].

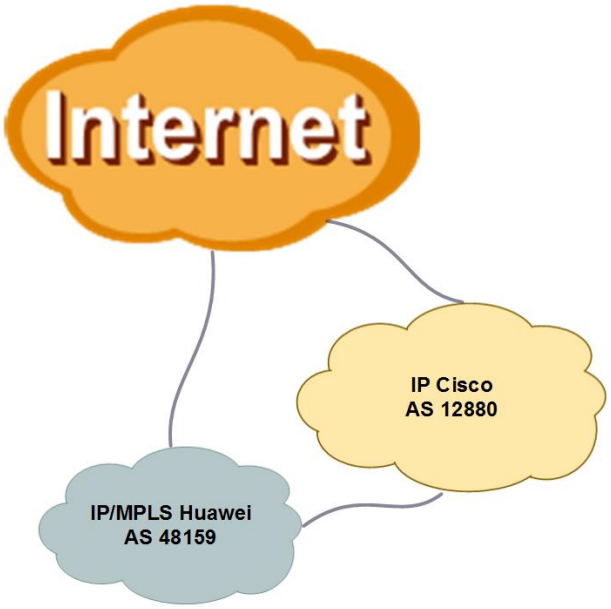
شبکه‌ی هسته در دو لایه‌ی انتقال و دیتا قابل بیان می‌باشد. در لایه‌ی دیتا عمدتاً کار مسیریابی در شبکه انجام می‌شود و در این بخش تجهیزات بررسی‌کننده‌ی بسته‌ها در لایه‌ی سوم شبکه قرار می‌گیرد. لایه‌ی انتقال می‌تواند در بخش‌های مختلف با استفاده از فناوری‌های مختلف اعم از فیبر نوری، انتقال رادیویی و انتقال ماهواره‌ای پیاده‌سازی شود. از طرفی در هسته شبکه، پهنای باند وسیعی مورد نیاز است به همین منظور فناوری مخابرات نوری در هسته پیاده‌سازی می‌شود و فناوری‌های رادیویی و ماهواره‌ای به عنوان پشتیبان مورد استفاده قرار می‌گیرند.

شرکت ارتباطات زیرساخت به عنوان بخش backbone و یا ستون فقرات زیرساخت ارتباطی، تامین‌کننده‌ی ارتباطات بین‌استانی و همچنین ارتباطات بین‌الملل می‌باشد. بخش هسته، شامل لایه‌ی فیزیکی، لایه انتقال، لایه IP و همچنین لایه ارتباطات بین‌الملل کشور می‌باشد. در لایه فیزیکی هیچ‌گونه سرویسی به اپراتورها یا متقاضیان شرکت زیرساخت داده نمی‌شود. در لایه انتقال شرکت زیرساخت، چندین شبکه با فناوری‌های مختلف وجود دارد که از جمله‌ی این فناوری‌ها TDM، OTN و SDH می‌باشد. در شبکه TDM سرویس نقطه به نقطه با پهنای باند 2Mbps جهت ارتباطات بین‌استانی ارائه می‌گردد. لایه IP بخش هسته، در حال حاضر از دو شبکه مجزا تشکیل شده است:

(۱) شبکه IP که مبتنی بر تجهیزات سیسکو است.
(۲) شبکه IP/MPLS که مبتنی بر تجهیزات هواوی است.

این دو شبکه در کنار هم مشغول به فعالیت هستند و هرکدام مشتریان خود را سرویس‌دهی می‌نمایند. به طور کلی، ارتباط این دو شبکه به‌صورت شکل ۴ است.

هر کدام از این دو شبکه (سیسکو و هواوی) مشتریان خود را سرویس‌دهی می‌نمایند. برای مثال یک فراهم‌کننده‌ی سرویس اینترنت می‌تواند بنا بر تشخیص خود و بسته به نوع و بزرگی و اهمیت آن، به یکی از دو شبکه‌ی سیسکو یا هواوی متصل گردد؛ اما بیشتر مشتریان بزرگ مانند اپراتورهای موبایل (همراه اول، ایرانسل، رایتل، ...) و نیز ارائه‌دهندگان خدمات اینترنت (شاتل، پارس آنلاین، ...)، به هر دو شبکه‌ی سیسکو و هواوی به طور همزمان و به صورت Dual Home متصل هستند تا علاوه بر توزیع بار ترافیک خود بین دو شبکه، بتوانند



شکل ۴. ارتباط شبکه هسته با اینترنت [۴]

جدول ۴. ارزش گذاری شبکه هسته

شبکه هسته	محرمانگی	دسترسی‌پذیری	یکپارچگی
	۳	۳	۳

در صورت قطعی یا خرابی یک ارتباط، از بستر شبکه‌ی دیگر استفاده نمایند و درنتیجه دسترس‌پذیری سرویس‌های خود را بالا ببرند.

۲.۱.۵ ارزیابی مخاطرات شبکه هسته

در بخش هسته زیرساخت ارتباطی ۱۵۳ تهدید و آسیب‌پذیری به یکدیگر نگاشت شده‌اند و بر اساس احتمال وقوع این تهدیدات، تأثیر این نگاشت‌ها بر سه پارامتر محرمانگی، یکپارچگی و دسترسی‌پذیری مورد بررسی قرارگرفته است و در نهایت میزان پارامتر ضربه و مقدار مخاطره به ازای هر یک از نگاشت‌ها محاسبه شده است که نمونه‌ای از فرایند تحلیل مخاطره برای این ماژول در جدول ۵ ذکر شده است.

۳.۱.۵ تحلیل مدیریتی شبکه هسته

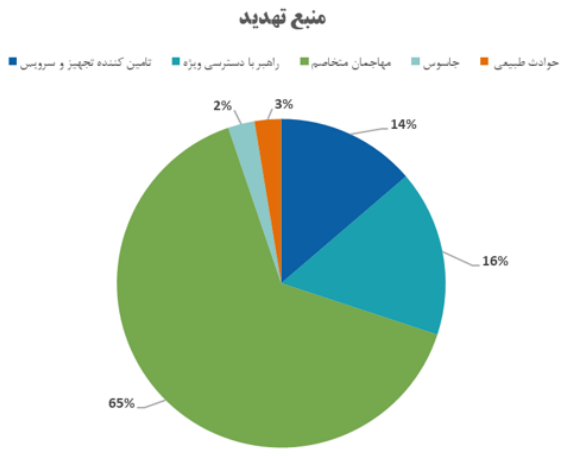
در بخش تحلیل مدیریتی دارایی، دارایی مربوطه از سه منظر فراوانی انواع تهدید، منبع تهدید و استراتژی برخورد مورد بررسی قرار می‌گیرد. شبکه هسته، از منظر ارزش، یکی از مهم‌ترین داریی‌های زیرساخت ارتباطی کشور محسوب می‌گردد، چرا که طبق استعلام از مالکان دارایی، در هر سه جنبه در دسترس بودن (A)، صحت (I) و محرمانگی (C)، بیشترین ارزش (امتیاز ۳) را به خود اختصاص داده‌اند، که این نشان از اهمیت این دارایی برای زیرساخت ارتباطی کشور دارد.

شکل ذیل فراوانی انوع تهدید در شبکه هسته را نمایش می‌دهد. از مجموع ۱۵۳ تهدید احصا شده شبکه هسته، همانگونه که در شکل ۵

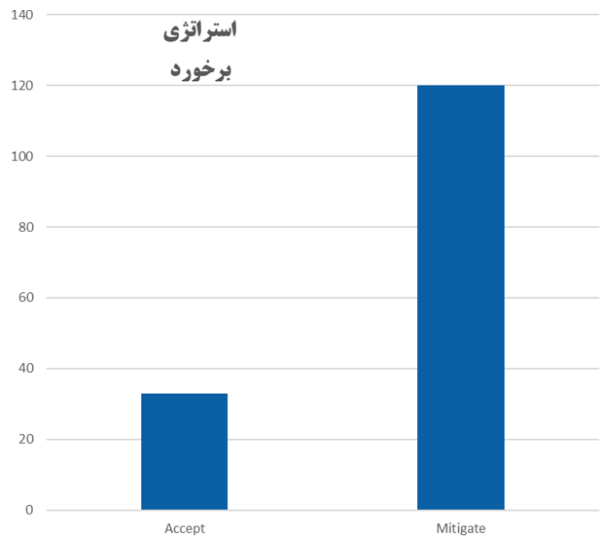
جدول ۵. ارزش‌گذاری شبکه هسته

ردیف	فهرست تهدیدات	منبع تهدید	نوع تهدید	احتمال وقوع	آسیب‌پذیری مرتبط با تهدیدات	ارزش آسیب‌پذیری	اثر بر روی در دسترس بودن	اثر بر روی محرمانگی	اثر بر روی صحت	ضربه	مخاطره	استراتژی برخورد
۱	شناسایی و اسکن وضعیت شبکه هسته	مهاجمان متخاصم	نشت اطلاعات	زیاد	عدم یا ضعف تجهیزات و سامانه تشخیص و جلوگیری از نفوذ در شبکه	زیاد	۰	۱	۰	۳	۲۷	Mitigate
۲	شناسایی و اسکن وضعیت شبکه هسته	مهاجمان متخاصم	نشت اطلاعات	زیاد	امکان نصب تجهیزات اسکن در روی تجهیزات مخابراتی و ارتباطی	متوسط	۰	۱	۰	۳	۱۸	Mitigate
۳	جمع‌آوری اطلاعات شبکه از منابع عمومی قابل دسترس	مهاجمان متخاصم	نشت اطلاعات	زیاد	عدم یا ضعف سیستم کنترل دسترسی و اعطای مجوز	زیاد	۰	۱	۰	۳	۲۷	Mitigate

شکل ۵. فراوانی انواع تهدیدی در شبکه هسته



شکل ۶. فراوانی منابع تهدید در شبکه هسته



شکل ۷. فراوانی استراتژی برخورد در شبکه هسته

هم مشخص است، تهدیدات اختلال در سیستم‌های اطلاعاتی، سرقت اطلاعات و حملات سایبری به ترتیب با ۲۲، ۱۸ و ۱۷ تکرار، پرتکرارترین تهدیدات متصور برای این دارایی می‌باشند.

شکل ۶ فراوانی منابع تهدید در شبکه هسته را نمایش می‌دهد. همانگونه که در شکل ذیل مشخص است، مهاجمان متخاصم با اختلاف، بیشترین منبع تهدید (۶۵٪) برای دارایی شبکه هسته محسوب می‌گردند. راهبر با دسترسی ویژه (تهدیدات داخلی) با ۱۶٪ و تامین کننده تجهیز و سرویس با ۱۴٪ نیز در رتبه‌های دوم وسوم منابع تهدید شبکه هسته قرار می‌گیرند.

شکل ۷ که مبتنی بر تحلیل مخاطرات به دست آمده، فراوانی استراتژی برخورد در شبکه هسته را نمایش می‌دهد. با توجه به ارزش بالای دارایی و نوع مخاطرات مرتبط، برای ۱۲۱ سناریوی مخاطره، استراتژی کاهش مخاطره و تنها برای ۳۲ سناریو، استراتژی پذیرش اتخاذ می‌گردد.

منظور از فراوانی استراتژی برخورد، پذیرش یا کاهش تهدید مربوطه

است. بحث پذیرش برای تهدیداتی مطرح می‌شود که ملاحظات و بسترسازی‌های اولیه مانند تمهیدات کنترل‌گری پیامدهای آن تهدید در دستور کار سازمان یا جامعه هدف قرار گرفته است و لذا تهدید جدی محسوب نمی‌شوند اما کاهش تهدید، استراتژی است که برای تهدیدات جدی و خطرساز مفروض می‌گردد که به دلیل شدت اثر، گریزی از برخورد با آن نیست.

۲.۵ تحلیل مخاطرات زیرساخت ابری

به منظور تحلیل مخاطرات ماژول زیرساخت ابری، شناخت این شبکه لازم است. لذا پس از مروری به وضعیت زیرساخت ابری، به تحلیل مخاطرات این شبکه پرداخته خواهد شد.

۱.۲.۵ شناخت زیرساخت ابری

رایانش ابری مدلی است که امکان دسترسی به محض تقاضا، فراگیر و آسان را به منابع محاسباتی قابل پیکربندی مشترک فراهم می‌سازد (مانند شبکه‌ها، سرورها، حافظه، برنامه‌های کاربردی و سرویس‌ها) که این منابع می‌تواند با کم‌ترین تلاش مدیریتی یا تعامل با فراهم‌کننده سرویس، به سرعت فراهم و در دسترس قرار گیرد. مدل ابر متشکل از پنج مشخصه اصلی، سه مدل سرویس و چهار مدل پیاده‌سازی است.

از منظر معماری در رابطه با چگونگی شباهت و تفاوت ابر با مدل‌های محاسباتی موجود سردرگمی وجود دارد و اینکه چگونه این شباهت‌ها و تفاوت‌ها باعث ایجاد رویکردهای فناوری، عملیاتی و سازمانی برای شبکه و امنیت اطلاعات می‌شوند. در واقع تفاوت بسیار ظریفی بین مدل محاسباتی مرسوم و رایانش ابری وجود دارد. با این وجود رایانش ابری منجر به رویکردهای فناوری، عملیاتی و سازمانی بسیار خوبی برای امنیت اطلاعات، امنیت شبکه و امنیت داده می‌شود. در حال حاضر تعریف‌های زیادی موجود است که تلاش می‌کنند تا ابر را از منظر دانشگاهیان، معماران، مهندسان، توسعه‌دهندگان، مدیران و مصرف‌کنندگان بررسی کنند. رایانش ابری را می‌توان به سه نوع کلی طبقه‌بندی کرد:

- ابر عمومی به مدلی از رایانش ابری اشاره دارد که در آن خدمات فناوری اطلاعات از طریق اینترنت ارائه می‌شود. به عنوان محبوب‌ترین مدل خدمات رایانش ابری شناخته شده، ابر عمومی انتخاب‌های گسترده‌ای از نظر راه‌حل‌ها و منابع محاسباتی برای رفع نیازهای روزافزون سازمان‌ها در هر اندازه‌ای ارائه می‌دهد.
- ابر خصوصی به هر راه‌حل ابری اطلاق می‌شود که برای استفاده توسط یک سازمان اختصاص داده شده است. در ابر خصوصی بر خلاف ابر عمومی، شما منابع رایانش ابری را با هیچ سازمان دیگری به اشتراک نمی‌گذارید و تفاوت اصلی در اینجاست. منابع دیتا سنتر ممکن است در محل زندگی افراد قرار داشته باشند یا توسط یک شرکت شخص ثالث در خارج از کشور اداره شوند. منابع محاسباتی ایزوله شده و از طریق یک شبکه خصوصی امن تحویل فرد داده می‌شوند و با مشتریان دیگر به اشتراک گذاشته نمی‌شوند.

جدول ۶. ارزش‌گذاری شبکه هسته

زیرساخت ابری	محرمانگی	دسترسی‌پذیری	یکپارچگی
	۳	۳	۳

- ابر ترکیبی هر محیط زیرساخت ابری است که بسترهای ابر عمومی و خصوصی را با هم ترکیب می‌کند و تفاوت‌های جزئی دارد. منابع معمولاً به عنوان یک محیط زیرساخت یکپارچه تنظیم می‌شوند. برنامه ها و حجم کاری داده‌ها می‌توانند منابع را بین استقرار ابر عمومی و خصوصی بر اساس سیاست‌های تجاری و فنی سازمانی حول جنبه‌هایی مانند زیر تنظیم کنند:
  - امنیت
  - کارایی
  - مقیاس‌پذیری
  - هزینه
  - بهره‌وری

این یک مثال رایج از ابر ترکیبی است: سازمان‌ها می‌توانند از محیط‌های ابری خصوصی برای بار کاری فناوری اطلاعات خود استفاده کنند و زیرساخت را با منابع ابری عمومی تکمیل کنند تا جهش‌های گاه به گاه در ترافیک شبکه را تطبیق دهند یا شاید از ابر عمومی برای حجم کاری و داده‌هایی که حساس نیستند استفاده کنند و در هزینه صرفه‌جویی کنند، اما ابر خصوصی را برای داده‌های حساس انتخاب می‌کنند.

در نتیجه، دسترسی به ظرفیت محاسباتی اضافی نیازی به CapEx بالای یک محیط ابری خصوصی ندارد، بلکه به عنوان یک سرویس فناوری اطلاعات کوتاه مدت از طریق یک راه‌حل ابر عمومی ارائه می‌شود. خود محیط به طور یکپارچه برای اطمینان از عملکرد بهینه و مقیاس‌پذیری برای تغییر نیازهای کسب وکار یکپارچه شده است.

۲.۲.۵ ارزیابی مخاطرات شبکه زیرساخت ابری

در بخش زیرساخت ابری زیرساخت ارتباطی ۱۱۰ تهدید و آسیب‌پذیری به یکدیگر نگاشت شده‌اند و بر اساس احتمال وقوع این تهدیدات، تأثیر این نگاشت‌ها بر سه پارامتر محرمانگی، یکپارچگی و دسترسی‌پذیری مورد بررسی قرار گرفته است و در نهایت میزان پارامتر ضربه و مقدار مخاطره به ازای هر یک از نگاشت‌ها محاسبه شده است که نمونه‌ای از فرایند تحلیل مخاطره برای این ماژول در جدول ۷ ذکر شده است.

۳.۲.۵ تحلیل مدیریتی زیرساخت ابری

در بخش تحلیل مدیریتی دارایی، دارایی مربوطه از سه منظر فراوانی انوع تهدید، منبع تهدید و استراتژی برخورد مورد بررسی قرار می‌گیرد.

زیرساخت ابری، از منظر ارزش، یکی از مهم‌ترین داریی‌های شبکه ملی اطلاعات محسوب می‌گردد، چرا که طبق استعلام از مالکان دارایی، در هر سه جنبه در دسترس بودن (A)، صحت (I) و محرمانگی (C)،

جدول ۷. نمونه‌ای از تحلیل مخاطرات زیرساخت ابری

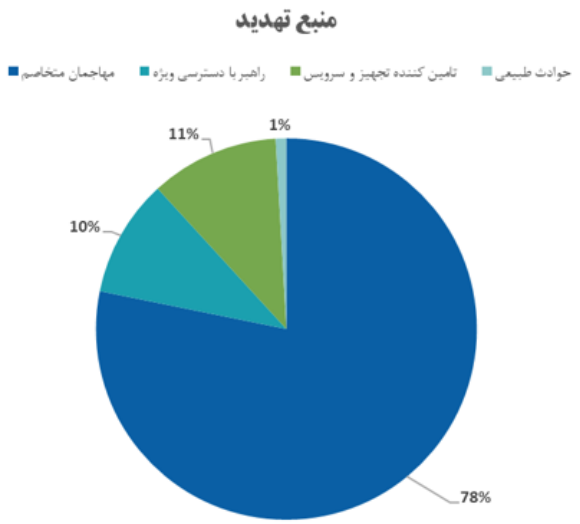
ردیف	فهرست تهدیدات	منبع تهدید	نوع تهدید	احتمال وقوع	آسیب‌پذیری مرتبط با تهدیدات	ارزش آسیب‌پذیری	اثر بر روی در دسترس بودن	اثر بر روی محرمانگی	اثر بر روی صحت	ضربه	مخاطره	استراتژی برخورد
۱	شناسایی و اسکن وضعیت شبکه ارتباطی زیرساخت‌های ابری	راهبر با دسترسی ویژه	نشت و سرقت اطلاعات	زیاد	امکان نصب نرم‌افزارهای اسکنر برروی سرورهای مدیریتی	متوسط	۰	۱	۰	۳	۱۸	Mitigate
۲	شناسایی و اسکن وضعیت شبکه ارتباطی زیرساخت‌های ابری	راهبر با دسترسی ویژه	نشت و سرقت اطلاعات	زیاد	عدم یا ضعف در کنترل دسترسی و اعطای دسترسی بیش از حد	زیاد	۰	۱	۰	۳	۲۷	Mitigate
۳	جمع‌آوری اطلاعات وضعیت شبکه زیرساخت‌های ابری از منابع عمومی قابل دسترس	مهاجمان متخاصم	نشت و سرقت اطلاعات	متوسط	عدم رعایت سطوح محرمانگی اطلاعات در انتشار	متوسط	۰	۱	۰	۳	۱۲	Mitigate
۴	جمع‌آوری اطلاعات وضعیت شبکه زیرساخت‌های ابری از منابع عمومی قابل دسترس	تأمین‌کننده تجهیز و سرویس	نشت و سرقت اطلاعات	متوسط	به اشتراک گذاری اطلاعات طبقه‌بندی شده شبکه به پیمانکاران	زیاد	۰	۱	۰	۳	۱۸	Mitigate

شکل ۸. فراوانی انواع تهدید در زیرساخت ابری

بیشترین ارزش (امتیاز۳) را به خود اختصاص داده‌اند، که این نشان از اهمیت این دارایی برای شبکه شما دارد.

شکل ذیل فراوانی انوع تهدید در زیرساخت ابری را نمایش می‌دهد. از مجموع ۱۱۰ تهدید احصا شده زیرساخت ابری، همانگونه که در شکل ۸ هم مشخص است، تهدیدات آلوده شدن سیستم توسط کدهای مخرب، حملات سایبری، سرقت و نشت اطلاعات به ترتیب با ۳۴، ۱۶ و ۱۶ تکرار، پرتکرارترین تهدیدات متصور برای این دارایی می‌باشند.

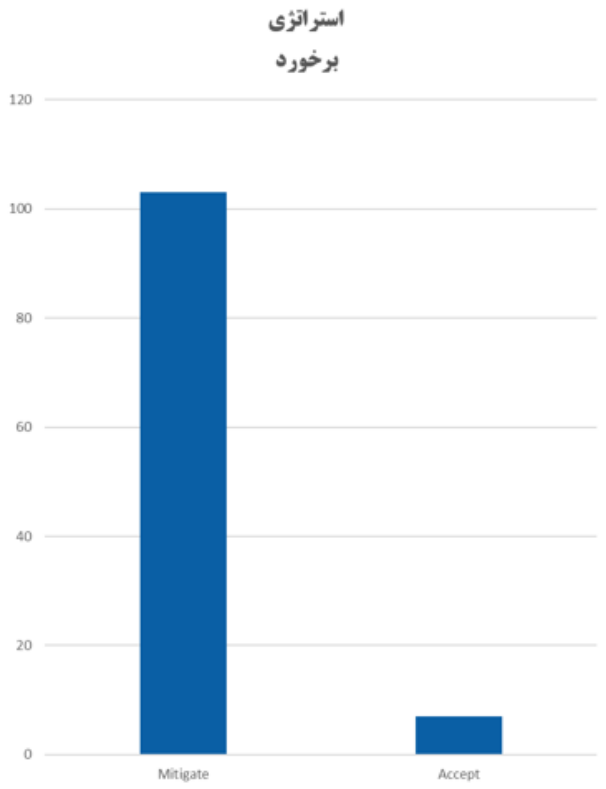
شکل ۹ فراوانی منابع تهدید در زیرساخت ابری را نمایش می‌دهد. همانگونه که در شکل ذیل مشخص است، مهاجمان متخاصم با اختلاف، بیشترین منبع تهدید (۷۸٪) برای دارایی زیرساخت ابری محسوب می



شکل ۹. فراوانی منابع تهدید در زیرساخت ابری

گردند. تأمین‌کننده تجهیز و سرویس با ۱۱٪ و راهبر با دسترسی ویژه (تهدیدات داخلی) با ۱۰٪ نیز در رتبه‌های دوم و سوم منابع تهدید زیرساخت ابری قرار می‌گیرند.

شکل ۱۰ مبتنی بر تحلیل مخاطرات صورت پذیرفته، فراوانی استراتژی برخورد در زیرساخت ابری را نمایش می‌دهد. با توجه به ارزش بالای دارایی و نوع مخاطرات مرتبط، برای ۱۰۳ سناریوی مخاطره، استراتژی



شکل ۱۰. فراوانی استراتژی برخورد در زیرساخت ابری

کاهش مخاطره و تنها برای ۷ سناریو، استراتژی پذیرش اتخاذ می‌گردد.

۶ ارائه الزامات امنیتی زیرساخت ارتباطی و اطلاعاتی

در طرح بررسی امن‌سازی زیرساخت کشور، پس از شناسایی دارایی‌های زیرساخت‌های ارتباطی و اطلاعاتی و تحلیل مخاطرات مرتبط با آن، نیاز به تدوین الزامات و کنترل‌های امنیتی مرتبط با هر یک از دارایی‌های این زیرساخت است. این بخش به تشریح برخی از این الزامات و کنترل‌های امنیتی مذکور می‌پردازد.

برای تدوین الزامات و کنترل‌های امنیتی، از چارچوب‌ها، استانداردها و به روش‌های مطرح دنیا در حوزه امنیت اطلاعات و نیز پژوهش‌ها و گزارش‌های پیشین در خصوص زیرساخت‌های ارتباطی و اطلاعاتی کشور بهره گرفته شده است. ابتدا به تفکیک هر دارایی، الزامات اختصاصی آن دارایی‌ها با دسته‌بندی‌های کاربردی ارائه گردیده و در انتهای گزارش، با بررسی ۳ چارچوب و استاندارد معتبر دنیا در حوزه امنیت اطلاعات، نگاشتی بین کنترل‌های اشاره شده در آن‌ها صورت پذیرفت. الزامات عمومی گزارش حاضر، از کنترل‌های نگاشت شده بین این ۳ چارچوب و استاندارد، تدوین و احصا شده است.

- ISO/IEC 27002:2022
- NIST SP 800-53
- CIS Control Version 8

به منظور ارائه دسته‌بندی موثرتر، الزامات حاضر در این بخش، چهار دسته‌بندی مختلف با چهار نگاه مختلف دسته‌بندی گردیدند که همه این دسته‌بندی‌ها از منابع معتبر امنیتی احصا گردیده است. در این دسته‌بندی علاوه بر نگاه خاصی که براساس سه استاندار فوق انجام گرفته کنترل‌های مرتبط با احصاء شاخص‌های سه‌گانه امنیت CIA نیز لحاظ شده است. با داشتن این دسته‌بندی‌ها، الزامات گزارش حاضر می‌تواند بر حسب نیاز کارفرما، انتخاب و به کارگیری شوند که این دسته‌بندی‌ها در گزارش الزامات امنیتی مربوط به خروجی‌های پروژه تدوین طرح جامع امنیت زیرساخت کشور [؟ ؟] گردآوری شده‌اند.

۱.۶ الزامات امنیتی شبکه هسته

در شبکه هسته از مجموع ۱۶۲ تهدید احصا شده شبکه هسته تهدیدات اختلال در سیستم‌های اطلاعاتی، حملات سایبری، سرقت و نشت اطلاعات به ترتیب با ۱۸، ۲۳ و ۱۷ تکرار، پرتکرارترین تهدیدات متصور برای این دارایی هستند. منابع تهدید در شبکه هسته مهاجمان متخاصم با اختلاف، بیشترین منبع تهدید (۶۵٪) برای دارایی شبکه هسته محسوب می‌گردند. راهبر با دسترسی ویژه (تهدیدات داخلی) با ۱۶٪ و تأمین‌کننده تجهیز و سرویس با ۱۴٪ نیز در رتبه‌های دوم و سوم منابع تهدید شبکه هسته قرار می‌گیرند. در ذیل نیز مخاطرات بر اساس اولویت برای شبکه هسته ذکر شده است.

در این بخش با توجه به تحلیل مخاطرات انجام شده، ۷۷ الزام خاص برای ماژول هسته ارائه شده است که برخی از این الزامات مرتبط در جدول ؟؟ ذکر شده است. الزامات بیشتر در سند [۹] گردآوری شده‌اند.

۲.۶ الزامات امنیتی زیرساخت ابری

در بخش زیرساخت ابری از مجموع ۱۱۰ تهدید احصا شده زیرساخت ابری تهدیدات آلوده شدن سیستم توسط کدهای مخرب، حملات سایبری، سرقت و نشت اطلاعات به ترتیب با ۳۴، ۱۶ و ۱۶ تکرار، پرتکرارترین تهدیدات متصور برای این دارایی می‌باشند. منابع تهدید در زیرساخت ابری مهاجمان متخاصم با اختلاف، بیشترین منبع تهدید (۷۸٪) برای دارایی زیرساخت ابری محسوب می گردند. تأمین‌کننده تجهیز و سرویس با ۱۱٪ و راهبر با دسترسی ویژه (تهدیدات داخلی) با ۱۰٪ نیز در رتبه‌های دوم وسوم منابع تهدید زیرساخت ابری قرار می‌گیرند.

در این بخش با توجه به تحلیل مخاطرات انجام شده، ۸۳ الزام خاص برای ماژول زیرساخت ابری ارائه شده است که برخی از این الزامات مرتبط در جدول ۸ ذکر شده است. الزامات بیشتر در سند [۹] گردآوری شده‌اند.

۷ نتیجه گیری

بر اساس آنچه که در ابتدای مقاله بیان شد، هدف این مقاله ارائه روشی تلفیقی در پارامترهای درگیر در محاسبه مخاطره که به سه شیوه کیفی، کمّی

جدول ۸. نمونه‌ای از الزامات امنیتی شبکه هسته

ردیف	الزام/کنترل امنیتی شبکه هسته	خانواده الزام/کنترل	دامنه عملیاتی	محور دفاعی	مخاطره مربوطه	تأثیر بر CIA	مرجع
۱	باید فایروال‌ها برای جلوگیری از دسترسی غیرمجاز به شبکه استفاده گردد که قابلیت فیلترکردن ترافیک شبکه را بر اساس آدرس‌های IP، پورت‌ها و پروتکل‌ها را داشته باشد.	فناورانه	حفاظت از سیستم‌ها، ارتباطات و اطلاعات	محافظت	دسترسی غیرمجاز به سیستم‌های اطلاعاتی	CIA	NIST 800-53
۲	باید از VPN برای ایجاد یک تونل رمزگذاری‌شدن بین دو اپراتورها استفاده شود. (بین لایه / بین مؤلفه)	فناورانه	حفاظت از سیستم‌ها، ارتباطات و اطلاعات	محافظت	نشت و سرقت اطلاعات	CI	NIST 800-53
۳	ترافیک شبکه باید کنترل و مانیتور شود تا فعالیت‌های مشکوک در شبکه شناسایی شوند و رویدادها به مرکز SOC ارسال شوند. (بین لایه / بین مؤلفه)	فناورانه	حفاظت از سیستم‌ها، ارتباطات و اطلاعات	محافظت	حملات سایبری	CIA	NIST 800-53
۴	برای محافظت از شبکه در برابر حملات امنیتی و مشکلات عملکردی باید نرم‌افزارها و سیستم‌عامل تجهیزات شبکه به‌روز نگه داشته شود.	فناورانه	حفاظت از سیستم‌ها، ارتباطات و اطلاعات	محافظت	حملات سایبری	CI	NIST 800-53
۵	باید بر روی کلیه سرورها و ایستگاه‌های کاری باید ضد بدافزار مناسب و قابل اطمینان نصب و بروز گردد.	فناورانه	حفاظت از سیستم‌ها، ارتباطات و اطلاعات	محافظت	آلوده‌شدن سیستم توسط کدها مخرب	CIA	NIST 800-53
۶	باید از احراز هویت دوعاملی برای امن‌سازی بستر ترافیک شبکه بین اپراتورها استفاده شوند. (بین لایه / بین مؤلفه)	فناورانه	شناسایی و احراز هویت	محافظت	نشت و سرقت اطلاعات	CA	NIST 800-53
۷	کلیه تجهیزات شبکه از جمله روترها و سوئیچ‌ها باید از RADIUS برای احراز هویت همه کاربران استفاده کنند. هیچ حساب کاربری محلی بر روی تجهیزات شبکه نباید پیکربندی شود.	فناورانه	مدیریت پیکربندی	محافظت	دسترسی غیرمجاز به سیستم‌های اطلاعاتی	C	Cisco Safe Document
۸	باید رمز عبور فعال روی روتر یا سوئیچ در یک فرم رمزگذاری‌شده ایمن نگهداری و بررسی تجهیزات تنظیم گردد.	فناورانه	مدیریت پیکربندی	محافظت	دستکاری یا حذف اطلاعات	C	Cisco Safe Document
۹	برای جلوگیری از حملات DoS و بهبود عملکرد شبکه باید IP directed broadcasts بر روی روتر یا سوئیچ غیرفعال گردد.	فناورانه	مدیریت پیکربندی	محافظت	اختلال یا از دسترس خارج‌شدن سرویس	A	Cisco Safe Document
۱۰	باید رمز عبور بر روی تجهیزات شبکه به صورت رمزگذاری فعال گردد.	فناورانه	مدیریت پیکربندی	محافظت	دسترسی غیرمجاز به تجهیزات	CA	Cisco Safe Document

و نیمه کمّی قابل محاسبه هستند می‌باشد. در این مستند برای اولین بار تحلیل مخاطره زیرساخت کشور از تلفیق هر سه روش استفاده شده است. بر این اساس بیش از ده‌ها سناریوی تهدید بر اساس نظرات خبرگی در این حوزه طراحی گردید که همزمان با ارزش‌گذاری دارایی توسط خبرگان تلفیق شد که در نهایت با بهره‌گیری از این دادگان کمّی و کیفی، نتایج و نمودارهای خوبی حاصل گردید.

این روش از آن جهت حائز اهمیت است که می‌تواند با دادگان متفاوت مانند ابزاری برای تحلیل مخاطرات مرتبط با موضوع عمل کند. روش‌شناسی این مستند براساس سنجش نظرات خبرگان یا proof of concept (POC) شکل گرفته و استخراج شاخص ها و استدلال‌ها هم بر این اساس انجام گرفته است و استخراج شاخص‌ها و استدلال‌ها در این مقاله بر اساس روش‌شناسی سنجش نظرات خبرگی است و validation یا verification آن هم مبتنی بر آن است که روش صحیحی برای تحلیل در این حوزه است.

هر چند که این مقاله از ادبیات استاندارد استفاده نموده و مدل‌سازی ندارد ولی از چارچوب و بازنمایی برخوردار است، زیرا تاکنون تحلیل مخاطرات زیرساخت کشور با تلفیق هر سه روش کمی کیفی و نیمه کمی در این سطح و قلمرو از دادگان انجام نگرفته و این کار برای اولین بار خود یك نوآوری یا نوپدیدی قلمداد می‌گردد. تمامی مقالاتی که در حوزه تحلیل مخاطره مورد مطالعه این مستند بوده در این قلمرو و با این وسعت از دادگان عمل نکرده و با تلفیق سه روش کمی، کیفی و نیمه‌کمی انجام نشده است. در این راستا توجه داورین محترم را به این نکته جلب می‌نماید که انتخاب روش‌شناسی ناشی از محدودیت تست عملی و قلمروی وسیع دادگان و عدم امکان رتبه‌بندی مخاطرات بوده اما در نهایت تأیید متولیان امر درخصوص خروجی‌ها نشان داده که انتخاب روش‌شناسی در این مستند موفق عمل کرده است.

همچنین در این مقاله تلاش شده تا خلاصه‌ای از روند تحلیل مخاطرات ماژول‌های زیرساخت ارتباطی و اطلاعاتی کشور مورد بررسی قرار گیرد و در نهایت فرمت الزاماتی امنیتی که برای این زیرساخت‌ها تعریف می‌گردد ارائه شود که در قالب نمونه‌ای از این فرایند برای ماژول‌های

زیرساخت هسته و زیرساخت ابری ارائه گردید. لازم به ذکر است که این مقاله مستخرج از پروژه ای است که در سال ۱۴۰۲ در پژوهشگاه فناوری اطلاعات با کد ۹۱۴۰۱۰۵۱۰ با ارزیابی ۹۷ درصد به انجام رسیده است و امکان ارائه اطلاعات بیشتر بر اساس درخواست رسمی از پژوهشگاه برای متقاضیان فراهم می‌باشد.

مراجع

[۱] سند تبیین الزامات شبکه ملی اطلاعات، مصوبه جلسه ۳۵ شورای عالی فضای مجازی.

[2] https://www.nist.gov/cyberframework

[۳] سند معماری و طرح کلان شبکه ملی اطلاعات، مصوبه جلسه ۶۶ شورای عالی فضای مجازی.

[۴] پروژه تدوین برنامه توسعه و تکامل شبکه ملی اطلاعات، سازمان فناوری اطلاعات و ارتباطات، ۱۳۹۷.

[۵] پروژه مشاوره و طراحی کلان و تفصیلی معماری امنیت، پژوهشگاه فناوری ارتباطات و اطلاعات، ۱۳۹۴.

[6] Derakhshandeh, Sadegh, and Nasser Mikaeilvand. "New framework for comparing information security risk assessment methodologies." Australian Journal of Basic and Applied Sciences 5.9 (2011): 160-166.

[۷] گزارش پیوست امنیتی شبکه ملی اطلاعات؛ پژوهشگاه فناوری ارتباطات و اطلاعات، ۱۳۹۴.

[۸] روش‌های ارزیابی آسیب‌پذیری زیرساخت‌ها و مدیریت بحران، شهرام علمداری و حسن مشهدی، چاپ سوم، ۱۳۹۸.

[۹] سند الزامات امنیتی شبکه ملی ،مستخرج از پروژه تدوین طرح جامع امن‌سازی زیرساخت شبکه، پژوهشگاه فناوری ارتباطات و اطلاعات، ۱۴۰۲.

[۱۰] گزارش بررسی و انتخاب متدولوژی تحلیل مخاطرات کشور، مستخرج از پروژه تدوین طرح جامع امن‌سازی زیرساخت شبکه، پژوهشگاه فناوری ارتباطات و اطلاعات، ۱۴۰۲.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2024, Volume 22, Number 1 (pp. 74–88)
https://monadi.isc.org.ir

The method of analyzing the risks of communication and information infrastructure modules and extracting preventive security requirements

Nasrin Taaj *, Amir Mansour Yadegari, Abouzar Arabsorkhi and Reza Kalantari

Information and Communication Technology Research Institute, Tehran, Iran

ARTICLE INFO.

Article history:
Received: May 7, 2024
Accepted: September 25, 2024
Published Online: October 28, 2024

Keywords:
Threats and vulnerabilities
Risk analysis method
Source and type of threats
Security requirements

Type: Research paper

ABSTRACT

According to the approvals of the Supreme Council of Cyberspace, the development of the country's infrastructure as an independent, safe, and stable infrastructure is one of the strategic priorities of the country, the realization of which, in addition to the technological requirements the field of information and communication technology, provides a platform for the establishment and development and supply of all kinds of services and content of the country's cyberspace; It is also necessary to provide safe and stable communication of the country's vital infrastructures. Based on the conceptual model contained in the resolution of the 66th meeting of the Supreme Council of Cyberspace, the communication and information infrastructure of the country consists of a series of main modules, whose risk analysis is in line with the reversibility of incidents, protection against threats, monitoring and intelligent response from the basic needs of achieving to safe and secure communications. Due to the space limitations of this article, the author intends to describe how to achieve risk analysis based on a combination of qualitative, quantitative, and semi-quantitative methods, some examples of these basic modules, and then, based on the results, how to exploit the emerging knowledge. Explain in the form of a diagram to identify the type of threat and its source and extract the aforementioned preventive security requirements.

© 2024 ISC

* Corresponding author
Email addresses: n_taj@itrc.ac.ir (Nasrin Taaj), amyadegari@itrc.ac.ir (Amir Mansour Yadegari), abouzar_arab@itrc.ac.ir (Abouzar Arabsorkhi), kalantar@itrc.ac.ir (Reza Kalantari)
© 2024 ISC. All rights reserved.