مدیریت ریسک در سامانهٔ جویش‌گرهای بومی

مهسا امیدوار سرکندی*[1]، نسرین تاج نیشابوری[2]، حسن کوشککی[3] و شقایق نادری[4]

[1، 2 و 3]پژوهشکدهٔ امنیّت مرکز تحقیقات مخابرات ایران، تهران، ایران
mahsa.omidvarsarkandi@gmail.com
n_taj@itrc.ac.ir
hassan.kooshkaki@gmail.com

[4]عضو هیأت علمی مرکز تحقیقات مخابرات، پژوهشکده امنیت، تهران، ایران
naderi@itrc.ac.ir

چکیده

امروزه سامانهٔ جویش‌گرهای بومی را یکی از شاخص‌های توسعهٔ صنعت فناوری اطلاعات در همهٔ کشورها می‌توان به‌شمار آورد. به همین دلیل موضوع ایمن‌سازی این نوع سامانه‌ها، با توجّه به جایگاه ویژهٔ آن‌ها در تأمین دست‌یابی کاربران به اطّلاعات درست در کم‌ترین زمان ممکن، مطرح می‌شود. مؤثرترین اقدامات برای تأمین امنیّت این نوع برنامه‌های کاربردی، انجام ارزیابی و مدیریت ریسک مطابق مرحلهٔ آغازین فرایند امنیت نرم‌افزار است. این اقدامات متشکل از مجموعهٔ مراحلی است که یک تیم نرم‌افزاری را در زمینهٔ مدیریت برنامه‌های کاربردی در طی فرایند توسعه یاری می‌دهد. برای کاهش سطح ریسک در این نوع سامانه‌ها، رویکرد پاسخ به ریسک انتخاب شده‌است. هدف اصلی این مقاله ارزیابی و مدیریت ریسک مطابق با اطلاعات جمع‌آوری‌شده بر مبنای پرسش‌نامهٔ طراحی‌شده است. همچنین برای شناسایی ریسک‌های مهم از روش‌شناسیNIST و کنترل‌های امنیتی استفاده و نتایج محاسبات سطح ریسک‌های مهم نیز به تفکیک حوزه‌های شناخته‌شده ارائه شده‌است.

واژگان کلیدی: سامانهٔ جویش‌گرهای بومی، ارزیابی و مدیریت ریسک، روش‌شناسیNIST، ریسک، تهدید

۱- مقدمه

امروزه سامانهٔ جویش‌گرهای بومی را پایهٔ توسعهٔ فناوری ارتباطات و اطلاعات و یکی از شاخص‌های توسعه‌یافتگی صنعت فناوری اطلاعات در همه کشورها می‌توان به‌شمار آورد. با آنکه کاربران، جویش‌گرها را بیش‌تر با جستجوی وب می‌شناسند، اهداف و کاربردهای بسیار گسترده‌تری دارند که جستجوی وب تنها یکی از آن‌ها به‌شمار می‌رود. جویش‌گرهای بومی با دانش و شناخت بیش‌تر نسبت به زبان مادری یک کشور و بهره‌مندی از ابزارهای پردازش زبان بومی و دسترسی بهتر به زبان‌شناسان آن کشور قابلیت مانور بیش‌تری در رفع نیازهای مردم آن کشور در حوزهٔ جستجوی وب دارند. همین عامل موجب شده‌است که سامانهٔ جویش‌گرهای بومی در تعدادی از کشورهای مطرح دنیا به موفقیت‌های بسیاری دست یابند. ازاین‌رو موضوع ایمن‌سازی این نوع سامانه‌ها، با توجّه به اهمیت و جایگاه ویژهٔ آن‌ها در تأمین دستیابی کاربران به اطلاعات درست در کم‌ترین زمان ممکن، مطرح می‌شود.

مؤثرترین اقدامات برای تأمین امنیّت این نوع برنامه‌های کاربردی، ارزیابی و مدیریت ریسک مطابق مرحله آغازین فرایند امنیت نرم‌افزار است. این مقاله به مدیریت ریسک در سامانهٔ جویش‌گرهای بومی متناسب با روش‌شناسی انتخاب‌شده و نیز ارائهٔ راهکارهای عمومی برای کاهش سطح ریسک می‌پردازد. موفقیت‌آمیزبودن انطباق میان مدیریت ریسک با پروژهٔ نرم‌افزار [۱]، مهم‌ترین دلیل محدودکردن مدیریت ریسک به سامانهٔ جویش‌گرهای بومی است. از سویی دیگر، اهمیّت ارزیابی ریسک در این نوع سامانه‌ها به‌گونه‌ای است که یک پیش‌نیاز برای مدیریّت رخدادها [1]به‌شمار می‌رود[۲]. همچنین نوع مدیریت ریسک در سه دستهٔ کلیِ: سطح سازمانی، سطح اهداف و فرآیندهای کسب و کار، و

[1] Incident Handeling

سامانه‌های اطلاعاتی[۳] طبقه‌بندی می‌شود که فرایند ارزیابی و مدیریت ریسک در قالب دستهٔ سوم به‌صورت زیر سازمان‌دهی شده‌است:

۱- شناخت و معرفی انواع ریسک؛

۲- معرفی مدیریت و ارزیابی ریسک در سامانه‌های جویش‌گر بومی؛

۳- استفاده از راهبرد پاسخ به ریسک به همراه روش‌شناسی NIST[1]؛

۴- بررسی نتایج حاصل از ارزیابی، ارزش‌گذاری ریسک و ارائهٔ کنترل امنیتی عمومی در سامانهٔ جویش‌گرهای بومی.

۲- شناخت ریسک و انواع آن

احتمال ازبین‌رفتن محرمانگی[2]، تمامیت[3] و دسترس‌پذیری[4] در اثر خطر یا تهدید[5]، ریسک معرفی شده‌است[۴]. همچنین، در تعریفی دیگر ریسک به‌عنوان رخدادی برای سنجش آن بر اساس معیار کیفی کم، متوسط و بالا ارزیابی شده‌است. طبقه‌بندی کلی ریسک‌ها به‌صورت زیر آورده شده‌است:

۱. ریسک‌های موقتی: ریسک‌هایی که با گذشت زمان به‌دلیل ایجاد تغییرات در محیط امنیتی تغییر می‌کنند و تغییرات ایجادشده در آن‌ها وابستگی مستقیم به تغییر در آسیب‌پذیری خاصی ندارد؛

۲. ریسک‌های وابسته: شدت این نوع ریسک‌ها، وابسته به میزان اهمیتی است که یک ریسک در مقایسه با سایر ریسک‌ها در یک محیط خاص دارد؛ به‌عنوان مثال، ریسک‌هایی که چندین عامل تهدیدکننده در به‌وجودآمدن و تشدید آن‌ها مؤثّر است، در مقایسه با سایر ریسک‌ها اهمیّت بالاتری دارند[۴]؛

همچنین از دیدگاهی دیگر، ریسک‌ها در حوزهٔ توسعهٔ برنامه‌های کاربردی در قالب دسته‌های زیر قرار می‌گیرند:

۱. ریسک‌های پروژه: ریسک‌هایی هستند که طرح پروژه را به مخاطره می‌اندازند؛

۲. ریسک‌های‌فنی: ریسک‌هایی هستند که کیفیت و موعد زمانی نرم‌افزار توسعه‌یافته را به خطر می‌اندازند.

۳. ریسک‌های کسب‌وکار: ریسک‌هایی که ماندگاری نرم‌افزار در دست توسعه را تحلیل می‌کنند. این مدل ریسک‌ها به‌طورمعمول پروژه و محصول را به خطر می‌اندازند؛

۴. ریسک‌های شناخته‌شده: ریسک‌هایی هستند که پس از ارزیابی دقیق طرح پروژه، محیط‌های فنی و تجاری توسعه پروژه و منابع اطلاعاتی قابل اعتماد کشف می‌شوند؛

۵. ریسک‌های قابل پیش‌بینی: ریسک‌هایی هستند که از تجارب گذشته کشف می‌شوند؛

۶. ریسک‌های غیر قابل پیش‌بینی: احتمال وقوع این نوع ریسک‌ها وجود دارد؛ اما تشخیص پیشاپیش آن‌ها بسیار مشکل است.

در این مقاله، سامانهٔ جویش‌گرهای بومی بر اساس ریسک‌های شناخته‌شده، بررسی و ارزیابی شده‌اند.

۳- مدیریت ریسک

فرایند شناسایی، ارزیابی و طی مراحلی برای کاهش ریسک، مدیریت ریسک شناخته می‌شود[۵]، همچنین انتخاب رویکرد مدیریت ریسک مناسب، فرایندها، روش‌ها، ابزارها، نقش و وظایف تیم‌ها را در پروژه‌ای خاص مشخص می‌سازد. از جمله اهداف مدیریت ریسک به جلوگیری از اتلاف هزینه، شناسایی و برنامه‌ریزی برای کاهش ریسک‌های فنی می‌توان اشاره کرد. به همین دلیل محاسبه و دسته‌بندی ریسک‌ها به میزان شناسایی و طبقه‌بندی آسیب‌پذیری‌های حوزهٔ سامانهٔ جویش‌گرهای بومی اهمیت دارد. شکل (۱) به دسته‌بندی رویکرد پاسخ به ریسک اشاره می‌کند که در این مقاله از میان چهار روش شناخته‌شدهٔ مدیریت ریسک (استفاده از فهرست کنترلی، استفاده از چارچوب تحلیلی، استفاده از مدل‌های فرایندگرا و راهبرد پاسخ به ریسک)، روش چهارم به‌دلیل جامعیت و نداشتن محدودیت‌های فهرست کنترلی در سامانهٔ جویش‌گرهای بومی انتخاب شده‌است[۶]. در ادامه به شرح مختصر هر یک از رویکردها پرداخته شده‌است:

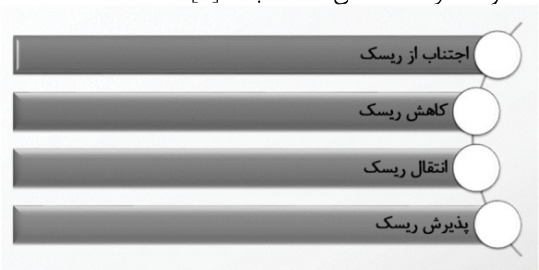
۱. اجتناب از ریسک: هدف از این راهبرد جلوگیری از وقوع تأثیرات منفی در پروژه، مانند تغییر در طراحی سامانه است.

۲. کاهش ریسک: به یک یا چند اقدام طراحی‌شدهٔ مستحکم برای کاهش تهدیدها از طریق کاهش تأثیرات و احتمال ریسک، قبل از یافتن آن اطلاق می‌شود.

[1] National Institute of Standards and Technology
[2] Confidentiality
[3] Intigrity
[4] Availibility
[5] Threat

۳. انتقال ریسک: این راهبرد شامل انتقال مسئولیت مدیریت و هدایت ریسک به شخص ثالث می‌شود. این روش، ریسک‌ها را کاهش نمی‌دهد، بلکه رسیدگی به آن به فرد دیگری واگذار می‌شود.

۴. پذیرش ریسک: این رویکرد شامل دامنهٔ وسیعی از راهبردهای فعال و غیرفعال می‌شود. در پذیرش غیرفعال ریسک، فرد با استفاده از برنامه‌های نظارتی، این نوع سامانه‌ها را می‌تواند کنترل و پایش کند. این روش زمانی مناسب است که تعداد تهدیدها کم و منبع ریسک خارج از محدودهٔ مشخص سامانه باشد[۶].



(شکل-۱): ارتباط رویکردهای کلی مدیریت ریسک

برای آنکه لزوم مدیریت ریسک مشخص شود، ابتدا لازم است به سه مرحله از مدیریت ریسک که در تمام روش‌شناسی‌ها مشترک است، اشاره شود:

۱- مرحلهٔ نخست: ارزیابی ریسک[1] نام دارد که در این مرحله ابتدا تمامی دارایی‌های موجود در دامنهٔ کاری سامانه شناسایی شده، سپس آسیب‌پذیری و تهدیدهای مربوط به هر دارایی شناسایی و درجه‌بندی می‌شود. این تهدیدها یک آسیب‌پذیری[2] را در سامانه می‌توانند فعال کرده و باعث ایجاد اختلال در عملکرد آن شوند. پس از شناسایی این تهدیدها باید نقاط آسیب‌پذیر سامانه به تفکیک هر دارایی شناسایی شود.

۲- مرحلهٔ دوم: کاهش ریسک[3]نام دارد که در این مرحله تأثیر ریسک بر سامانه و همچنین تواتر برخورد با ریسک باید کاهش یابد. از جمله راه‌های کاهش ریسک به موارد زیر می‌توان اشاره کرد:

۲-۱- ازبین‌بردن عامل بروز ریسک: در اینجا برای تبیین بهتر موضوع مثالی مطرح می‌شود: وجود یک یا چند صفحهٔ آسیب‌پذیر در سامانه احتمال امکان سوءاستفاده را از آن مهاجم افزایش می‌دهد و وی می‌تواند به سامانه نفوذ کند.

[1] Risk Assessment
[2] Vulnerability
[3] Risk Mitigation

تهدید و آسیب‌پذیری در این سناریو به‌صورت زیر می‌تواند موردتوجه قرار گیرد:

- تهدید: نفوذ کاربران غیر مجاز یا مهاجمان.
- آسیب‌پذیری: وجود حفرهٔ امنیتی در صفحات.

۲-۲- انتقال ریسک: به معنای واگذاری انجام کار یا مسئولیت آن به مرجع دیگری در خارج از سامانه است تا مسئولیت ریسک متوجه آن مرجع شود. به‌عنوان مثال، در این نوع سامانه‌ها که خرابی سرویس‌دهنده یکی از تهدیدهای جدّی تلقی می‌شود، با واگذاری امور نگهداری و تعمیر آن به یک پیمانکار خارجی، درعمل ریسک مربوط به این دارایی به وی منتقل می‌شود.

۳- مرحلهٔ سوم: ارزشیابی ریسک[4] نام دارد که در آن میزان کاهش ریسک با توجه به اقدامات انجام‌شده در مرحلهٔ قبل بررسی می‌شود. بنابراین مقایسه میان شاخص‌های طراحی‌شده با محاسبهٔ این شاخص‌ها قبل و بعد از مدیریت ریسک به‌دست‌آمده، ضروری است. اگر تعداد وقوع ریسک و یا شدت اثر آن بر سامانه کاهش یافته‌باشد، این به معنای موفقیت در فرایند مدیریت ریسک است. باید توجه داشت که احتمالات هم یک تهدید می‌تواند باشد و فقط نباید بر اساس حوادث رخ‌داده تصمیم گرفته شود. اگر احتمال وقوع حادثه برای دارایی‌های شناسایی‌شدهٔ سامانه وجود داشته‌باشد، باید آن را نیز تهدید به‌شمار آورد و در چهارچوب مدیریت ریسک، راه حل مناسبی برای آن در نظر گرفت. بر اساس نتایج به‌دست‌آمده در ارزیابی ریسک، باید واکنشی مناسب طراحی و اجرا شود. به عبارت دیگر، هدف از ارزیابی ریسک، ارزیابی دانش موجود در طراحی سامانه و کمینه نیازهای امنیتی به‌دست‌آمده از فرآیند طبقه‌بندی امنیتی برای تعیین اثر آن‌ها به‌منظور کاهش خطرات پیش‌بینی شده است.

موفقیت در حوزهٔ مدیریت ریسک، وابسته به مشارکت همه جانبهٔ ذی‌نفعان باتجربه و آگاه در این حوزه اعم از کاربران نهایی، کارشناسان فناوری اطلاعات و ارتباطات است که منجر به ارائهٔ تصویر جامع‌تری از تهدیدها و آسیب‌پذیری‌ها به‌منظور کاهش خطرات پیش‌بینی‌شده می‌شود [۷]. از میان روش‌شناسی‌های گوناگون مطرحی مانند Danger Matrix، Ra2وNIST برای مدیریت ریسک، NIST به‌دلیل جامعیت و

[4] Risk Evaluation

پیاده‌سازی آسان انتخاب شده‌است. تمامی این روش‌شناسی‌های شناخته‌شده، علاوه بر اینکه باید الزامات استاندارد را پوشش دهند، باید از دو ویژگی بسیار مهم نیز برخوردار باشند. این دو ویژگی عبارتند از:

- قابل‌مقایسه‌بودن: با به‌کارگیری این روش‌شناسی ریسک‌ها را به‌صورت کمی(قابل اندازه‌گیری) می‌توان تبدیل کرد. در این حالت با مقایسهٔ ریسک‌ها با یکدیگر و با درنظرگرفتن معیارهای سازمانی، برای طبقه‌بندی ریسک‌ها و درنهایت انتخاب راهکار کنترلی مناسب برای کاهش و کنترل ریسک می‌توان اقدام کرد.
- قابل‌تکراربودن: هر بار که ریسک‌های سامانه در شرایط یکسانی تحلیل و ارزیابی می‌شوند، انتظار می‌رود که نتایج با یک تقریب یکسان حاصل شوند. به‌عنوان‌مثال، اگر در ارزیابی انجام‌شده، ارزش یک ریسک در حد بالا[1] تشخیص داده شود، در ارزیابی دوباره نباید ارزش آن در محدودهٔ دیگری (به‌عنوان‌مثال حد پایین) تشخیص داده شود.

۴- مدیریت ریسک در سامانهٔ جویش‌گرهای بومی

روش‌شناسی NIST به‌عنوانِ یکی از مهم‌ترین روش‌شناسی‌های شناخته‌شده در مدیریت ریسک، هماهنگ با مدیریت امنیت اطلاعات[2] طراحی شده‌است. ISO [3] این روش‌شناسی را به‌عنوان کامل‌ترین روش‌شناسی معرفی کرده‌است. از میان نسخه‌های گوناگون آن، استاندارد NIST SP 800-64 [۹] چارچوب مدیریت ریسک را به‌کمک نقشه راه ساده و در قالب توابع امنیتی در فرایند توسعه نرم‌افزار[4] به‌طور کامل ترکیب می‌کند. ملاحظات امنیتی برای هر مرحله از فرآیند توسعهٔ نرم‌افزار در نظر گرفته شده‌است. بنابراین، کاربردهای کسب و کار و نیازمندی‌های امنیتی به‌طور هم‌زمان در طی این فرایند، پیشرفت داده‌می‌شوند تا توازن و تعادل میان این دو برقرار شود. در این مقاله سه گام اصلی مدیریت ریسک بر اساس روش‌شناسی NIST بررسی شده است. در مدیریت ریسک صرف‌نظر از نوع روش‌شناسی، باید ارزش‌گذاری ریسک به‌عنوان نخستین مرحله انجام شود. در این مرحله تمامی ریسک‌ها شناسایی، ارزش‌گذاری و اولویت‌بندی می‌شوند. در این روش‌شناسی، ارزش‌گذاری ریسک در نُه مرحلهٔ زیر طراحی شده‌است:

- مرحلهٔ نخست: تعریف بخش‌های سامانه[5]
- مرحلهٔ دوم: مشخص‌کردن تهدیدها[6]
- مرحلهٔ سوم: مشخص‌کردن آسیب‌پذیری‌ها[7]
- مرحلهٔ چهارم: تحلیل کنترل[8]
- مرحلهٔ پنجم: تشخیص میزان احتمال وقوع[9]
- مرحلهٔ ششم: تحلیل تأثیرات[10]
- مرحلهٔ هفتم: تشخیص ریسک[11]
- مرحلهٔ هشتم: توصیه‌های کنترلی[12]
- مرحلهٔ نهم: مستندسازی نتایج[13]

در ادامه به تشریح هریک از مراحل ارزش‌گذاری در مدیریت ریسک مطابق روش‌شناسی NIST پرداخته شده‌است.

۴-۱- مرحلهٔ نخست: تعریف بخش‌های سامانه

در این مرحله هدف، شناسایی دارایی‌هایی است که برای توسعهٔ برنامهٔ کاربردی تحت وبی مانند جویش‌گرهای بومی مهم و ارزشمند تلقی می‌شود و ضروری‌ست که ریسک‌های مرتبط با آن‌ها مدیریت شود. دارایی‌ها ممکن است، موارد ملموس، مانند عملیات و یا پایگاه‌داده‌های یک سامانه، یا به‌طورکامل ناملموس، مانند شهرت و اعتبار اجرایی یک سامانه یا سازمان باشد. هنگام امن‌سازی یک سامانه باید زیرساخت و برنامه‌های کاربردی را تجزیه و تحلیل و تهدیدهای بالقوه را شناسایی کرد. همچنین دارایی‌ها می‌بایست در محدوده و دامنهٔ امنیت اطلاعات سامانه[14] شناسایی شوند. سندی که در آن مرزهای امنیت اطلاعات سامانه مشخص شده، در این مرحله به‌عنوان ورودی محسوب می‌شود. موارد زیر مطابق با چهار بخش اصلی تشکیل‌دهندهٔ مشترک میان سامانهٔ جویش‌گرهای بومی؛ یعنی مؤلفهٔ نمایه‌ساز، مؤلفهٔ رتبه‌بند، مؤلفهٔ خزش‌گر و واسط کاربری[۱۱و۱۰]، به‌عنوان دارایی می‌توانند شناسایی شوند:

- تمامی نرم‌افزارها و سخت‌افزارها

[1] High
[2] Inforamtion Security Mnagement Systems(ISMS)
[3] International Standard Organization
[4] Software Development Life Cycle (SDLC)
[5] System Characterization
[6] Threat Identification
[7] Vulnerability Identification
[8] Control Analysis
[9] Likelihood Determination
[10] Impact Analysis
[11] Risk Determination
[12] Control Recommendations
[13] Results Documentation
[14] Scope

- اطلاعات و داده‌ها اعّم از اطلاعاتِ مشتریان، تأمین‌کنندگان و سایر ذی‌نفعان
- نیروهای انسانی اعّم از کاربران، عوامل پشتیبانی سامانه و مدیران که برای سامانه ارزشمند هستند.
- تمامی مستندات (درصورت موجودبودن) اعم از شیوه‌نامه‌ها، روش‌های اجرایی، آیین‌نامه‌ها، بخش‌نامه‌ها، قراردادها، سند، طرح شبکه، راهنمای کاربران، سند مربوط به توپولوژی شبکه، مستندات سامانهٔ مدیریت امنیت اطلاعات[1]
- مکان‌های نگهداری اطلاعات اعم از دیسک نرم، دیسک سخت
- تمامی نسخه‌های پشتیبانی
- سرویس‌های نصب‌شده بر روی رایانه‌ها اعم از سرویس رایانامه و سرویس نمابر
- کنترل‌های عملیاتی اعم از قفل‌ها، حفاظ پنجره‌ها، تأسیسات و سامانه‌های حفاظتی

توجه به این نکته ضروری‌ست که دارایی‌ها باید براساس شرایط سامانه توسعهٔ برنامهٔ کاربردی تحت وب شناسایی شود. به عبارت دیگر، اگر تجهیزات فیزیکی یک سامانه در شرایط محیطی سخت و در معرض رطوبت یا گرد و غبار قرار داشته‌باشد، معیار شناسایی دارایی‌ها متفاوت خواهدشد و مواردی همچون تأسیسات تهویهٔ مطبوع نیز چنانچه در محدودهٔ دامنهٔ امنیت اطلاعات سامانه به کار گرفته شده‌باشند، باید به‌عنوان دارایی شناسایی و به آن توجه شود، زیرا تأثیرات منفی هوای آلوده، رطوبت، گرد و غبار و مواد شیمیایی بر روی سامانه، باید کنترل شود. همچنین، شناسایی دارایی‌ها فقط محدود به زمان حال نیست و مواردی که به‌عنوان دارایی ممکن است در آینده در دامنهٔ امنیت اطلاعات سامانه به‌کار گرفته نیز باید شناسایی شوند؛ مانند سامانه‌های نرم‌افزاری که هنوز خریداری نشده‌اند، یا قرارداد آن منعقد شده، یا سامانه‌هایی که هنوز در مرحلهٔ طراحی قرار دارند. علاوه‌براین، بخش شبکه که به‌عنوان یک شریان اطلاعاتی مهم در توسعه و پیاده‌سازی سامانهٔ جویش‌گرهای بومی شناخته‌شده‌اند، در موضوع امنیت اطلاعات از اهمیت ویژه‌ای برخوردارند؛ بنابراین مستندات مربوط به شبکه از دارایی‌های مهم محسوب می‌شود.

سؤال‌هایی که در این بخش مطرح می‌شوند، به شرح زیراند:

۱-آیا طراحی مؤلفه‌های شبکهٔ آن متناسب با نیازمندی‌های مطالعه و استخراج‌شده انجام شده است؟

۲- آیا در هنگام نصب و نگهداری مؤلفه‌های شبکه مطابق الزامات امنیتی، دقت کافی و لازم انجام شده‌است؟

دارایی‌ها باید با جزئیات کامل شناسایی شوند، چراکه در معرض تهدیدقرارگرفتن آن‌ها و وجود آسیب‌پذیری می‌تواند کل کسب‌وکار را متوقف کند و قابلیّت دسترسی، تمامیت و محرمانگی را تحت‌الشعاع قرار دهد. توجّه به این نکته ضروری‌ست که پس از تشخیص فقدانِ حتی یک مورد از دارایی‌ها در تمام طول گام‌های نه‌گانه، آن را به فهرست دارایی‌ها می‌توان اضافه کرد و اجرای مرحلهٔ نخست نیز محدوده زمانی مشخصی ندارد.

۲-۴-مرحلهٔ دوم: مشخص‌کردن تهدیدها

در این مرحله، هدف شناسایی تهدیدها، منابع[2] و انگیزهٔ ایجاد تهدید[3] به تفکیک تک‌تک دارایی‌های شناسایی‌شده در مرحلهٔ نخست است. شناسایی تمام تهدیدها بالقوه صرف‌نظر از عمدی یا سهوی بودن و اینکه برای دارایی موضوعیت دارد یا خیر، باید با دقت انجام شود. میزان هر تهدید شناسایی‌شده برای دارایی‌ها، در مرحلهٔ سوم ارزشیابی ریسک بررسی خواهد شد. هم‌زمان با شناسایی تهدیدها، منبع یا منابع هر تهدید و همچنین مسائل انگیزشی هریک که منبع آن را برای ایجاد تهدید انگیزه‌مند می‌کند، باید در این مرحله شناسایی و در مراحل بعد (همان‌گونه که به آن اشاره خواهدشد) کنترل شود. توجه به این نکته لازم است که انگیزش منبع تهدید، تنها برای نیروی انسانی و آن هم در شرایط عامدانه مدنظر است. از دیگر موارد مهم در این مرحله، شناسایی دقیق عملکرد هر تهدید و آثار عملی‌شدن تهدید است که باید در این مرحله به آن توجه شود.

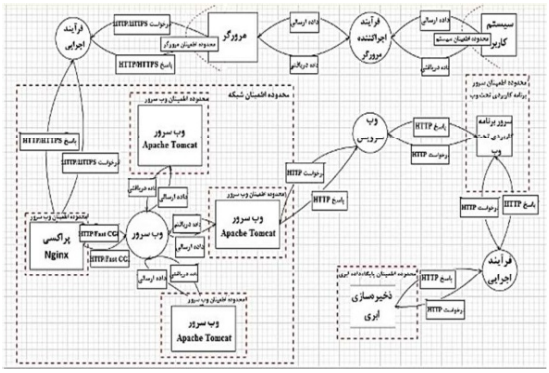
مجموعه تهدیدهای مهم از دیدگاه مهندسی نرم‌افزار مطابق با شکل (۲)، به‌کمک ابزار MicrosoftThreat Modeling 2016 [۱۲] و مبتنی بر شیوه STRIDE [۱۳و ۱۴] ، ترسیم و طراحی شده‌است، همچنین، این شکل نشان‌دهندهٔ نمونه‌ای از مؤلّفه‌های اصلی به‌کاررفته، تحت شبکه سامانه جویش‌گرهای بومی است که شامل سرویس‌دهنده‌های وب، برنامهٔ کاربردی و پایگاه‌داده می‌شود.

[1] Information Security ManagementSystem(ISMS)

[2] Threat Source

[3] Motivation

نحوهٔ قرار گرفتن و ارتباط میان مؤلفه‌های این سامانه برگرفته از معماری توزیع‌شده در حوزهٔ معماری نرم‌افزار است. مناطقی که با عنوان" محدودهٔ اطمینان" در شکل مشخص شده‌اند، مرز اعتماد میان مؤلفه‌های گوناگون با یک‌دیگر را نشان می‌دهند. به عبارت دیگر، تبادل و انتقال اطّلاعات میان این محدوده‌ها منوط به عبور از سطح دسترسی، تعریف و پیاده‌سازی شده‌است؛ همچنین، این ترسیم اهمیت بررسی و شناسایی تهدیدها شناخته‌شده در مرحلهٔ طراحی نرم‌افزار را نشان می‌دهد. این موضوع می‌تواند دربارهٔ شناسایی تهدیدها ناشناخته نیز به کار رود، اما دقیق نخواهدبود [۶]. انواع تهدیدها مطابق این رویکرد در قالب شش دستهٔ کلی: جعل اطلاعات، تحریف اطلاعات، انکار اطلاعات، افشا اطلاعات، ممانعت از سرویس و ارتقای مجوز دسترسی جای می‌گیرند؛ همچنین، از محدودهٔ اطمینان مشخص‌شده میان مؤلفه‌های این الگوسازی می‌توان در رویکرد دفاع در عمق[1]، استفاده کرد [۱۵].



(شکل-۲): الگوسازی تهدیدها سامانه جویش‌گرهای بومی

بر اساس پژوهش‌ها و ارزیابی‌های مبتنی بر روش جعبه سیاه[2]، مهم‌ترین تهدیدهای سامانه‌های جویش‌گر بومی در بخش رابط کاربری، مطابق با فهرست ده تهدید برتر OWASP هستند [۱۶]:

- پردازه‌گذاری فرا- وبگاهی[3]
- پیکربندی نادرست امنیتی[4]
- افشای اطلاعات حساس و مهم [5]

رفع این آسیب‌پذیری‌ها تأثیر مهمی در کاهش شدت ریسک‌های مرتبط دارد که در بخش ۳-۴ به آسیب‌پذیری‌های مرتبط با تهدیدهای شناسایی‌شده پرداخته شده‌است.

۳-۴- مرحلهٔ سوم: مشخص‌کردن آسیب‌پذیری‌ها

در این مرحله هدف شناسایی آسیب‌پذیری‌ها به‌تفکیک دارایی‌های شناسایی‌شده در دامنهٔ امنیت اطلاعات سامانه است. تهدیدها به‌تنهایی خطری ندارند؛ اما اگر از آسیب‌پذیری‌های موجود سوءاستفاده شود، به‌طور قطع سامانه را با خطر روبه‌رو خواهندکرد. آسیب‌پذیری به‌صورت عمدی و یا سهوی می‌تواند فعال شود. موضوع قابل توجّهِ دیگر، تفاوت میان مفهوم تهدید و آسیب‌پذیری است که نباید به‌جای یک‌دیگر استفاده شوند. آسیب‌پذیری مرتبط با سامانه است؛ اما تهدید صرف‌نظر از شرایط سامانه و نوع فعالیت آن، همواره در محیط وجود دارد؛ به‌عنوان مثال، از لحاظ امنیتی همواره به سازمان‌ها توصیه شده‌است که برای جلوگیری از هرگونه سوءاستفادهٔ احتمالی زمان ترک هریک از کارکنان (به هر دلیلی)، شناسه و گذرواژهٔ وی باید بلافاصله غیرفعال و حذف شود. حال، اگر چنین کاری به‌موقع انجام نشود، این مورد یک آسیب‌پذیری برای سامانهٔ مرتبط می‌تواند تلقی شود؛ اما تهدید متناظری هم وجود دارد و آن، احتمال واردکردن اطلاعات نادرست به سامانه یا نفوذ به آن با استفاده از گذرواژهٔ دیگران است. همچنین، آسیب‌پذیری‌های متناظر با دارایی‌هایی که ممکن است در آینده در دامنه امنیت سامانه‌های جویش‌گرهای بومی قرار گیرند، نیز باید شناسایی شوند؛ از جمله مشکلاتی که درخصوص شناسایی آسیب‌پذیری‌ها وجود دارد، فقدان دانش افرادی است که در این حوزه فعالیت می‌کنند؛ به‌عنوان مثال، برای تشخیص آسیب‌پذیری‌های دارایی‌هایی که سامانه‌ها هنوز در اختیار ندارند و در سال‌های آینده خریداری خواهندشد، هیچ شناختی از این دارایی‌ها در دست نیست. در چنین شرایطی توصیه می‌شود که از منابع شناخته‌شدهٔ موجود در سایر سامانه‌ها استفاده شود. گاهی تولیدکنندگان آسیب‌پذیری‌های محصولات خود را معرفی و در قالب بستهٔ به‌روزرسانی‌شده[6] به مشتریان عرضه می‌کنند. البته از مشکلات عمده نرم‌افزارهای ایرانی عدم وجود چنین امتیازی است. برای حل این مشکل، توصیه شده به آسیب‌پذیری‌های نرم‌افزارهایی مانند سامانهٔ جویش‌گرهای بومی توجه شود. آسیب‌پذیری همواره از سه زاویه باید شناسایی شوند:

[1] Defence in Depth
[2] BlackBox
[3] Cross-Site Scripting (XSS)
[4] Security Misconfiguration
[5] Sensitive Data exposure
[6] Update Pack

۱. مدیریتی: مثل امکان یا عدم‌امکان دسترسی به سامانه در زمان‌های مختلف، از جمله امکان دسترسی افراد غیرمجاز؛
۲. عملیاتی: اشتباه کاربران سامانه در اثر عدم‌آگاهی کافی آنها و ورود اطلاعات نادرست؛
۳. فنی: عدم‌دسترسی به اطلاعات فنی نرم‌افزار، تداخل نرم‌افزارهای مختلف که امنیت سامانه را به مخاطره اندازند؛ به این معنا که باید به دارایی‌های شناسایی‌شده از سه زاویهٔ بالا نگریسته‌شود. لازم است توجه شود که تهدیدها و آسیب‌پذیری‌ها همواره باید در محدودهٔ دامنه امنیت اطلاعات سامانه شناسایی و کنترل شوند. در غیر این صورت، ممکن است به اتلاف منابع و یا عدم‌استفادهٔ درست از آن‌ها منجر شود.

در جدول (۱) نتیجهٔ ارزیابی چهارده آسیب‌پذیری مهم سامانهٔ جویش‌گرهای بومی با راهنمای آزمون OWASP [۱۳]، طراحی و گردآوری شده‌است. یکی از بارزترین ویژگی‌های این جدول تجمیع شناسه‌های مرتبط با آسیب‌پذیری‌های مرتبط با ده تهدید برتر شناخته‌شده از مؤسسه‌های معتبر امنیت نرم‌افزار است، علاوه‌براین، بر اساس CVSS[1] مرتبهٔ اهمیت آن‌ها در این جدول درج شده‌است تا در ارزیابی ریسک از این مقدار برای محاسبه میزان ریسک استفاده شود.

۴-۴- مرحلهٔ چهارم: تحلیل کنترل

در این مرحله هدف، شناسایی کنترل‌های در حال اجرا در دامنهٔ امنیّت اطلاعات سامانه است. دلیل انجام این کار، شناسایی کنترل‌های موردنیاز برای مدیریت ریسک و با شناسایی کنترل‌های موجود است. مطابق روش‌شناسی NIST بهتر است، قبل از شناسایی کنترل‌های لازم، فهرستی از کنترل‌های درحال‌اجرا تهیه شود تا با به‌کارگیری کنترل‌های تکراری و توسعه سامانهٔ جویش‌گرهای بومی هزینهٔ اضافی تحمیل نشود؛ همچنین، در این بخش کنترل‌هایی که هنوز به اجرا درنیامده، اما برای اجرای آن برنامه وجود دارد نیز، باید شناسایی شوند. به‌عنوان مثال، ممکن است پنجره‌های اتاق سرور حفاظ نداشته باشد؛ اما برای ایجاد آن قراردادی منعقد شده و قرار باشد درنهایت تا یک‌ماه دیگر این حفاظ نصب شود. در این حالت حفاظ اتاق سرور به‌عنوان یک کنترل درحال‌اجرا شناسایی شود.

[1] Common Vulnerability Scoring System

زمانی که از شناسایی کنترل‌ها برای مدیریت ریسک سخن به میان می‌آید، لازم است این شناسایی به تفکیک کنترل‌های فنی و غیرفنی انجام شود. این کنترل‌ها برای سامانهٔ جویش‌گرهای بومی گوناگون، متفاوت است؛ اما به مهم‌ترین آن‌ها، همانند استفاده از ضدبدافزارها و غیرفعال‌کردن پورت‌های ورودیِ سرویس‌گیرنده‌ها می‌توان اشاره کرد و در زمینه کنترل‌های غیر فنی (مدیریتی) نیز به دستورالعمل‌ها و بخش‌نامه‌های مدیریتی برای استفادهٔ بهتر و کنترل‌شده از امکانات سامانه (مانند بخشنامهٔ اعمال محدودیت بر زمان استفاده از اینترنت و بخش‌نامهٔ ساختار رمزعبورها) می‌توان اشاره کرد. برای آشنایی بیش‌تر با کنترل‌ها به متن استاندارد ISO 27002مراجعه شود [۲۱-۲۳]. در این استاندارد تعداد ۱۳۳ کنترل به‌منظور اعمال مدیریت درست بر ریسک‌های شناسایی‌شده سازمان توسعه‌دهندهٔ سامانه، توصیه شده‌است. به‌کارگیری این ۱۳۳ کنترل در مدیریت ریسک الزامی نیست؛ اما برای مستثنی‌کردن هرکدام از آن‌ها باید دلیل قانع‌کننده‌ای ارائه شود.

۵-۴- مرحلهٔ پنجم: تشـــخیص میزان احتمال وقوع

در این مرحله هدف، ارزیابی و محاسبهٔ سطح تواتر وقوع هر ریسک است. در این مرحله سؤالات زیر مطرح می‌شود:

- میزان احتمال وقوع تهدید شناسایی‌شده چقدر است؟ (روزانه، ماهیانه، دو ماه یک‌بار)
- امکان تکرار وقوع این تهدید چقدر است؟
- تهدید شناسایی‌شده چقدر ممکن است از آسیب‌پذیری موجود سامانه استفاده کند و خطرساز شود؟

توجه به این نکته ضروری است که در این مرحله تنها میزان احتمال و تواتر وقوع ریسک بررسی می‌شود که برای محاسبهٔ آن از موارد زیر می‌توان استفاده کرد:

- مطالعه و بررسی سوابق ارزیابی‌های گذشته: نشان‌دهندهٔ رخ‌دادن سطح تواتر تهدیدها در گذشته است. به این منظور باید مستندات مستدلی برای نشان‌دادن وقوع تهدید موجود باشد. این مورد، همواره به‌عنوان اولویت نخست در ارزیابی و محاسبهٔ سطح تواتر وقوع ریسک، استفاده می‌شود. در صورت عدم‌کفایت مستندات در این بخش، بهتر است از نظر افراد خبره استفاده شود. از آنجا که از تاریخ آغاز بررسی

آسیب‌پذیری و تهدیدهای سامانهٔ جویش‌گرهای بومی، مستند دقیق و کاملی دربارهٔ سوابق تهدیدها شناسایی‌شده سامانهٔ جویش‌گرهای بومی گردآوری و تألیف نشده‌است، از مستندات" نقشهٔ راه امن‌سازی جویش‌گرهای بومی" در طرح پژوهشی انجام‌شده از تاریخ ۱۳۹۴/۶/۳۱ تا ۱۳۹۵/۱/۳۱ در پژوهشکدهٔ امنیت مرکز تحقیقات مخابرات ایران استفاده شده‌است و محوریت اصلی آن بررسی آسیب‌پذیری‌ها و تهدیدهای مهم بخش‌های گوناگون سامانهٔ جویش‌گرهای بومی است.

- بهره‌گیری از نظر افراد خبره، جنبهٔ دیگری است که برای ارزیابی و محاسبهٔ سطح تواتر وقوع ریسک و به‌منظور استفاده از نظرات و تجربیات اشخاص خبره مطرح می‌شود. موضوع حائز اهمیت در این زمینه، سابقه و سطح تحصیلات افراد شرکت‌کننده در نظرسنجی و در پی آن محرزشدن صلاحیت آن‌هاست. به‌منظور ارزیابی سطح تواتر وقوع ریسک باید خروجی حاصل از گام‌های دوم، سوم و چهارم به‌عنوان ورودی گام پنجم به‌دقت بررسی و تحلیل شود؛ چون خروجی گام‌های دوم، سوم و چهارم تأثیر زیادی در تعیین سطح تواتر وقوع ریسک دارد. در غیر این صورت، خروجی گام پنجم و درنهایت، نتیجهٔ ارزش‌گذاری ریسک قابل‌استناد نخواهدبود. معیارهای سنجش سطح تواتر وقوع ریسک باید به‌طور دقیق تعریف شوند. به‌عنوان مثال، معنای "درجه بالا" در عبارت" سطح تواتر وقوع ریسک بالا تعریف شده‌است" باید مشخص شود. پس از مشخص‌شدن منبع رخداد، در مرحله "تحلیل تأثیرات ریسک" با توجه به نتایج حاصل از مرحلهٔ دوم و سوم برای گردآوری اطلاعات کامل باید به خبرگان این حوزه مراجعه شود.

(جدول-۱): شناسهٔ آسیب‌پذیری‌های شناسایی‌شده مرتبط با سامانهٔ جویش‌گرهای بومی[۲۴-۴۶].

آسیب پذیری	آسیب پذیری در	Basic CVSS نمره	تاثیر در	ده تهدید برتر OWSAP 2013	SANS/CWE Top 25 2011	شناسه CAPEC[1]	شناسه CWE[2]	شناسه WASC[3]
Integer Overflows	سمت سرویس-دهنده[4]	۱۰	کد	-	۶۸۲	۱۲۸	۱۹۰	WASC-03
حفاظت ناکافی لایهٔ انتقال	سمت سرویس-دهنده	۴	مدیریتی	A6 – Sensitive Data Exposure	۳۱۹	-	۳۱۱ ، ۵۲۳	WASC-04
Format String	سمت سرویس-دهنده	۱۰	کد	-	-	۶۷	۱۳۴	WASC-06
سرریز حافظهٔ بافر	سمت سرویس-دهنده	۱۰	کد	-	۱۱۹	۱۰,۱۰۰	۱۲۰,۱۱۹	WASC-07
Cross Site Scripting (XSS)	سمت سرویس‌گیرنده[5]	۴/۶	کد	A3 – Cross-Site Scripting (XSS)	۷۹	۶۳,۱۹,۱۸	۷۹	WASC-08
منع خدمت	سمت سرویس-دهنده	۸/۷	مدیریتی	A7 – Missing Function Level Access Control	۴۰۴	۱۱۹	۴۰۰	WASC-10
جعل محتوا	سمت سرویس-گیرنده	۵	کد	A2- Broken Authentication and Session Management	-	۱۴۸	۳۴۵	WASC-12
نشت اطلاعات	سمت سرویس-دهنده	۵	مدیریتی	A5 – Security Misconfiguration	۲۰۹	۱۱۸	۲۰۰	WASC-13
پیکربندی نادرست سرویس‌دهنده	سمت سرویس-دهنده	۱/۵	مدیریتی	A5 – Security Misconfiguration	-	-	۱۶	WASC-14
پیکربندی نادرست برنامه کاربردی	سمت سرویس-دهنده	۱/۵	مدیریتی	A5 – Security Misconfiguration	-	-	۱۵	WASC-15

[1] Commom Attack Pattern Enumeration and lassification
[2] Common Weakness Enumeration
[3] Web Application Security Consertium

[4] Server
[5] Client

WASC-24	۹۳	۱۰۵	-	A3 – Cross-Site Scripting (XSS)	کد	۴/۶	سمت سرویس-گیرنده	HTTP Request Splitting
WASC-25	۱۱۳	۳۴	-	A1 – Injection	کد	۴/۶	سمت سرویس-گیرنده	HTTP Response Splitting
WASC-26	۴۴۴	۳۳	-	-	مدیریتی	۴/۶	سمت سرویس-گیرنده	HTTP Request Smuggling
WASC-27	۴۳۶	۲۷۳	-	-	مدیریتی	۴/۶	سمت سرویس-گیرنده	HTTP Response Smuggling
WASC-45	۲۰۵	۲۲۴	-	-	مدیریتی	۰	سمت سرویس-دهنده	بررسی/ شناسایی
WASC-47	۶۱۳	۶۰	۷۳۹	A2- Broken Authentication and Session Management	مدیریتی	۸/۶	سمت سرویس-دهنده	Insufficient Session Expiration

ارزیابی و محاسبهٔ سطح تواتر وقوع ریسک، در بیش‌تر موارد به‌صورت کیفی انجام می‌شود؛ اما اگر با استفاده از سازوکارهای منطقی بتوان آن را کمّی کرد، در افزایش دقت کار تأثیرگذار خواهدبود. روش‌شناسی NIST در مورد امتیازدهی توصیهٔ مشخصی ندارد؛ بنابراین تخصیص امتیاز در این مرحله تابع هیچ‌گونه قانونی نبوده، ابتکاری است و باید با در نظر گرفتن پایایی، معیاری برای امتیازدهی انتخاب شود؛ همچنین، در برخی موارد ضروری‌ست در ارزیابی و محاسبهٔ سطح تواترِ وقوع ریسک، از تخمین استفاده شود. این حالت بیش‌تر در مورد دارایی‌هایی رخ می‌دهد که قرار است در آینده در محدودهٔ دامنهٔ امنیت اطلاعات سامانه به‌کار گرفته‌شوند و هنوز شناخت دقیقی از آن‌ها وجود ندارد. به‌منظور تخمین سطح تواتر وقوع ریسک، در اختیار داشتن اطّلاعاتی مانند نظر افراد خبره، سوابق عملکرد دارایی‌ها و نظر شرکت سازنده اجتناب‌ناپذیر است.

۶-۴- مرحلهٔ ششم: تحلیل تأثیرات ریسک

هدف از این مرحله، ارزیابی و محاسبهٔ شدت اثر وقوع هر ریسک بر روی مؤلفه‌های سامانه‌های جویش‌گر بومی خواهدبود. برخی از سؤالات مطرح‌شده در این مرحله، به‌صورت زیر است:

- در اثر وقوع ریسک چه میزان از یک‌پارچگی سامانه کاهش خواهدیافت؟
- در اثر وقوع ریسک چه میزان از محرمانگی اطلاعات موجود در سامانه کاهش خواهدیافت؟
- در اثر وقوع ریسک چه میزان از دردسترس‌بودن اطلاعات موجود در سامانه کاهش خواهدیافت؟

سطح تواتر وقوع ریسک و شدت اثر آن دو مقولهٔ به‌طورکامل متفاوت و جدا از هم هستند. احتمال دارد یک ریسک در فواصل زمانی طولانی رخ دهد، اما شدت اثر کمی داشته‌باشد؛ مانند ویروسی‌شدن یک رایانه در یک کلاس آموزشی که ممکن است، روزانه رخ دهد؛ امّا این امر آموزش را به‌طور کامل مختل نمی‌کند. برخلاف آن، ممکن است، احتمال وقوع یک تهدید کم باشد، اما شدت اثر آن در سطح بالایی قرار داشته باشد. مانند انفجار در اتاق سرور سازمان که امکان وقوع آن کم است، اما اگر رخ دهد، تبعات ناگواری را به دنبال خواهد داشت؛ بنابراین، دو مقولهٔ میزان تکرار و تأثیر باید به‌صورت جداگانه، با دقّت و حساسیت ویژه‌ای محاسبه شوند. به‌منظور محاسبهٔ شدت اثر وقوع ریسک، بهتر است از سه زاویهٔ یک‌پارچگی، محرمانگی و دردسترس‌بودن به دارایی‌هایِ شناسایی‌شده در محدودهٔ دامنه امنیت اطلاعات سامانه نگریسته شود. در صورت امکان بهتر است، میزان کاهش موارد بالا به‌صورت کمّی محاسبه و ارزیابی شود. به این منظور و در صورت لزوم، شاخص‌های کمّی تعریف و میزان آن‌ها باید در فواصل زمانی تعریف‌شده محاسبه شود؛ اما در مواردی که محاسبه و ارزیابی کمّیِ شدت اثر وقوع ریسک میسر نباشد، ارزیابی باید به‌صورت کیفی انجام شود.

۶-۴-۱- ارزیابی ریسک سامانهٔ جویش‌گرهای بومی

به‌منظور محاسبهٔ سطح ریسک و تعیین درجهٔ اهمیت تهدیدها سامانهٔ جویش‌گرهای بومی (مطابق رابطهٔ محاسبهٔ ریسک که در ادامهٔ جدول (۲) آمده است)، لازم است، علاوه‌بر در اختیار داشتن تأثیر تهدیدها و میزان احتمال وقوع آن‌ها، اطلاعاتی از آسیب‌پذیری‌های این نوع سامانه‌ها مدّنظر قرار

گیرد. به این منظور پرسش‌نامه‌ای مطابق جدول (۲)، با هدفِ به‌دست‌آوردن یکی از مشخصه‌های رابطه محاسبهٔ ریسک در اختیار متولیان حوزهٔ توسعهٔ جویش‌گرهای بومی قرار گرفت. مقدار امتیاز درنظرگرفته شده برای این پرسش‌نامه به صورت زیر دسته‌بندی شده‌است:

۱- تهدیدهای با درجهٔ بالا (۱۰-۷): تأخیر در اعمال رویکردهای سریع ترمیم و یا عدم‌وجود برنامه‌ای برای مدیریت امنیت سامانه و اطلاعات آن، باعث افزایش شدت آثار مخرب خواهدشد. این سطح از تهدیدها و ریسک‌ها، خسارات جبران‌ناپذیری به سامانه وارد می‌کنند و تأثیر بسیار فراوانی در تحقّق نیازهای کارکردی مهم دارند؛ همچنین در بیش‌تر موارد احتمال تبدیل این‌گونه تهدیدهای بالقوه به حملات خطرناک بالاست.

۲- تهدیدهای با درجهٔ متوسط (۶-۴): اقدامات مناسب در بازهٔ زمانی مطلوب و کوتاه، برای این سطح از تهدیدها در سامانهٔ جویش‌گرهای بومی بسیار حائز اهمیت است و تأثیر زیادی در تحقّق نیازهای کارکردی مهم دارد؛ همچنین در برخی موارد احتمال تبدیل این‌گونه تهدیدهای بالقوه به حملات خطرناک متوسط است.

۳- تهدیدهای با درجه کم (۳-۱): این سطح از تهدیدها دارای تأثیرات و آثار تخریبی بسیار کم‌تری نسبت به سایر تهدیدها هستند و تأثیر کمی در تحقق نیازهای کارکردی مهم دارند. با اعمال صحیح الزامات امنیتی، می‌توان این درجه از تهدیدها را کاهش داد. همچنین احتمال تبدیل این‌گونه تهدیدهای بالقوه به حملات خطرناک کم است.

این پرسش‌نامه حاوی ۶۴ سؤال بوده و ساختار آن به‌گونه‌ای طراحی شده‌است که شامل هر دو جنبهٔ مهم مرتبط با ریسک (آسیب‌پذیری و تهدیدها) می‌شود. آسیب‌پذیری‌های درج‌شده در جدول، حاصل پژوهش‌های انجام‌شده بر روی سامانهٔ جویش‌گرهای بومی مطابق با راهنمای ارزیابی برنامه‌های کاربردی تحت وب OWASP[1] [۱۸] است. تهدیدهای مرتبط با این آسیب‌پذیری‌ها نیز در چهار سطح/حوزهٔ ارزیابی: رابط کاربردی (تهدیدهای وابسته به بخش کدنویسی و تهدیدهای وابسته به بخش تنظیمات مدیریتی و پیکربندی)، مرحلهٔ خزش‌گر، مرحلهٔ نمایه‌ساز و مرحلهٔ رتبه‌بند طبقه‌بندی شده‌اند. یادآوری می‌شود این پرسش‌نامه براساس مهم‌ترین موارد سطح/حوزه ارزیابی گردآوری شده‌است.

(جدول-۲): پرسش‌نامه معیارهای ارزیابی سامانه جویش‌گرهای بومی بر اساس تهدیدها و آسیب‌پذیری‌های استخراج‌شده

ردیف	سطح/ حوزه ارزیابی	پرسش‌های فنی- عملیاتی	ریسک محاسبه‌شده	میانگین
۱	واسط کاربری	آسیب‌پذیری وابسته به بخش کدنویسی		
۱-۱	Integer Overflows	با توجه به این‌که این آسیب‌پذیری باعث سرریز حافظه می‌شود و در دسترسی به حافظه اختلال ایجاد می‌کند، میزان اهمیت بررسی این موضع چقدر اولویت دارد؟	۵	۳/۸۴
۱-۲	Format String		۵/۷	
۱-۳	سرریز حافظه بافر[2]		۶	
۱-۴	Cross Site Scripting (XSS)	ازآن‌جایی که این آسیب‌پذیری در اثر اعتبارسنجی نادرست نقاط ورودی برنامه به وقوع می‌پیوندد، میزان اهمیت بررسی این موضوع چقدر اولویت دارد؟	۴/۰۵	
۱-۵	جعل محتوا[3]	با توجه به این امر که این آسیب‌پذیری منجر به تغییر غیرمجاز محتوای برنامه می شود، میزان اهمیت بررسی این موضوع چقدر اولویت دارد؟	۳	
۱-۶	HTTP Request Splitting	این آسیب‌پذیری ناشی از عدم‌تنظیم و یا عدم‌وجود ویژگی امنیتی برای بررسی ورودی و خروجی در استفاده از عنصر خاصی به نام CRLF [4] است. با توجه به	۲/۳	

[1] Open Web Application Security Project
[2] Buffer Overflow
[3] Content Spoofing
[4] Carriage Return Line Feeds

۱-۷	HTTP Response Splitting	موضوع بالا، میزان اهمیت بررسی این موضوع چقدر اولویت دارد؟ (میزان اهمیت هر یک را با امتیاز مشخص کنید).	۳/۴	
۲	واسط کاربری	آسیب‌پذیری وابسته به بخش تنظیمات مدیریتی و پیکربندی		
۲-۱	حفاظت ناکافی لایهٔ انتقال[1]	از آن جایی که ضعف در پروتکل‌های امنیتی، استفاده و پیاده‌سازی نادرست آن باعث نشت اطلاعات می‌شود، میزان اهمیت بررسی این موضوع چقدر اولویت دارد؟	۲/۷	۴/۱۰
۲-۲	منع خدمت[2]	با توجه به اهمیت این آسیب‌پذیری که ویژگی دسترس‌پذیری را هدف قرار می‌دهد، میزان اهمیت اقدامات امنیتی را برای کاهش این تهدید و آسیب‌پذیری‌های مرتبط با آن چگونه ارزیابی می‌کنید؟	۶	
۲-۳	نشت اطلاعات[3]	از آن جایی که در صورت عدم‌پیاده‌سازی دقیق و اصولی، مهاجمان قادر به دست‌یابی و سوءاستفاده از اطلاعات هستند، میزان اهمیت کلی را به‌منظور پیش‌گیری و کاهش تهدیدهای مرتبط با آن چگونه ارزیابی می‌کنید؟	۳/۳	
۲-۴	پیکربندی نامناسب سرویس‌دهنده[4]	از آن جا که تنظیمات نادرست سرویس‌دهنده، باعث سوءاستفادهٔ مهاجم و به‌دست‌آوردن کنترل آن می‌شود، میزان اهمیت این موضوع را چگونه ارزیابی می‌کنید؟	۵/۱	
۲-۵	پیکربندی نامناسب برنامه کاربردی[5]	با توجه به این‌که تنظیمات نادرست و نامناسب در سرویس‌دهندهٔ برنامهٔ کاربردی تحت وب، منجر به سوءاستفادهٔ کاربر و تهدیدی برای بخش اجرایی برنامه محسوب می‌شود، میزان اهمیت این موضوع را چگونه ارزیابی می‌کنید؟	۵	
۲-۶	HTTP Request Smuggling	با توجه به اهمیت موضوع تضمین یک‌پارچگی در ارسال و دریافت درخواست‌های کاربران، میزان اهمیت این موضوع را چگونه ارزیابی می‌کنید؟ (میزان اهمیت هر یک را با امتیاز مشخص کنید).	۵	
۲-۷	HTTP Response Smuggling		۴/۰۵	
۲-۸	بررسی/ شناسایی[6]	مهاجمان به‌منظور دست‌یابی به اطلاعات مهم برنامه‌های کاربردی تحت وب، به بررسی و شناسایی تمام بخش‌های برنامه‌ی کاربردی می‌پردازند. این اطلاعات در ادامه به اجرای سناریوهای مخرب مهاجمان می‌تواند کمک کند. با توجه به توضیحات بالا، میزان اهمیت این موضوع را چگونه ارزیابی می‌کنید؟	۰	
۲-۹	Insufficient Session Expiration	بخش قابل‌توجهی از حملات مرتبط با دسترسی به حساب کاربران است که از مهم‌ترین آن‌ها می‌توان به CSRF[7] اشاره کرد. با توجه به توضیحات بالا، میزان اهمیت انجام مجموعهٔ اقدامات کاهندهٔ تأثیرات این آسیب‌پذیری و تهدیدها را چگونه ارزیابی می‌کنید؟	۳/۴	

[1] Insuficient Transport Layer Protection
[2] Denial of Service
[3] Information Leakage
[4] Server Misconfiguration
[5] Application Misconfiguration
[6] Fingerprinting
[7] Cross- Site Request Forgery

۳	فاز خزش‌گر	آسیب‌پذیری وابسته به بخش مؤلفهٔ خزش‌گر		
۳-۱		در صورت وجود نقض یا پیاده‌سازی ضعیف، اهمیت سیاست انتخاب[1] را چگونه ارزیابی می‌کنید؟	۵/۱۶	
۳-۲		در صورت وجود نقض یا پیاده‌سازی ضعیف، اهمیت سیاست بازمشاهده[2] را چگونه ارزیابی می‌کنید؟	۴/۴۷	
۳-۳		در صورت وجود نقض یا پیاده‌سازی ضعیف، اهمیت سیاست موازی‌سازی[3] را چگونه ارزیابی می‌کنید؟	۳/۹۴	
۳-۴		در صورت وجود نقض یا پیاده‌سازی ضعیف، اهمیت سیاست ادب[4] را چگونه ارزیابی می‌کنید؟	۴/۸۵	
۳-۵		راهبردهای انتخاب محتوا (مثل حرکت بهترین آغاز، خزش‌گر متمرکز، خزش‌گر علمی متمرکز، خزش مسیر صعودی، محدودکردن پیوندها، نرمال‌سازی نشانی‌ها و غیره) که در سیاست انتخاب خزش‌گرها وجود دارد، تا چه میزان به پوشش و خزش صفحات وب (که با درخواست‌های کاربران ارتباط نزدیک دارد) می‌تواند کمک کند؟	۳/۹۷	
۳-۶		اهمیت تهدید حملات منع خدمت را چگونه ارزیابی می‌کنید؟	۳/۳۸	
۳-۷		اهمیت تهدید حملات تزریق کد به ربات‌های خزش‌گر را چگونه ارزیابی می‌کنید؟	۵/۱۹	۴/۳۴
۳-۸		اهمیت تهدید حملات روی پایگاه‌داده خزش‌گر (در صورت استفاده از پایگاه داده برای خزش‌گر) را چگونه ارزیابی می‌کنید؟	۲/۱۸	
۳-۹		اهمیت مقابله با عوامل طراحی ضعیف در خزش‌گر (مثل توازن بار خزش‌گر، پایداری خزش‌گر، پهنای باند، منابع پردازشی، منابع ذخیره‌سازی، الگوریتم‌های خزش و مسائل زیرساختی خزش‌گر) را چگونه ارزیابی می‌کنید؟	۳/۴۴	
۳-۱۰		اهمیت تهدیدهای تله‌اسپایدر و افتادن خزش‌گر را در حلقهٔ بی‌نهایت چگونه ارزیابی می‌کنید؟	۵/۵۳	
۳-۱۱		میزان اهمیت بررسی و مقابله با وب‌سایت‌های آلوده یا صفحات اسپم را در مرحلهٔ خزش‌گر چگونه ارزیابی می‌کنید؟	۳/۹۷	
۳-۱۲		میزان اهمیت درنظرگرفتن امنیت پهنای باند را در مرحلهٔ طراحی چگونه قلمداد می‌کنید؟	۲/۸۶	
۳-۱۳		میزان اهمیت درنظرگرفتن امنیت منابع پردازشی را در مرحلهٔ طراحی چگونه قلمداد می‌کنید؟	۴/۶۸	
۳-۱۴		میزان اهمیت درنظرگرفتن امنیت منابع ذخیره‌سازی را در مرحلهٔ طراحی چگونه قلمداد می‌کنید؟	۳/۸۱	
۴	مرحلهٔ نمایه‌سازی	آسیب‌پذیری وابسته به بخش مؤلفهٔ نمایه‌ساز		
۴-۱		تعیین و انجام دورهٔ به‌روزرسانی نمایه‌ساز تا چه میزان در کشف و مقابله با وب‌سایت‌های آلوده می‌تواند مؤثر باشد؟	۱/۵۳	
۴-۲		میزان اهمیت و مقابله با حملات پایگاه‌دادهٔ نمایه‌ساز(در مرحلهٔ نمایه‌سازی) را چگونه ارزیابی می‌کنید؟	۲/۰۸	۱/۹۸
۴-۳		میزان اهمیت و مقابله با حملات ماژول جستجو را (در مرحلهٔ نمایه‌سازی) چگونه ارزیابی می‌کنید؟	۱/۲۸	

[1] Selection Policy
[2] Re-visit Policy
[3] Parallelization Policy
[4] Politeness Policy

۴-۴		میزان اهمیت چالش‌های مربوط به موازی‌سازی فرایندها را در نمایه‌ساز (در مرحلهٔ نمایه‌سازی) چگونه ارزیابی می‌کنید؟	۲/۳۶	
۴-۵		میزان اهمیت چالش‌های مربوط به دورهٔ به‌روزرسانی نمایه‌ساز و رسیدن به یک مصالحهٔ زمانی (اگر این مورد به‌درستی پیاده‌سازی و تنظیم شود، فرایند کشف تارنماهای آلوده بهتر انجام می‌شود- در مرحلهٔ نمایه‌سازی) را چگونه ارزیابی می‌کنید؟	۱/۳۶	
۴-۶		تأثیر و اهمیت عوامل طراحی ضعیف را در نمایه‌ساز (تحمل‌پذیری خطا، مرحلهٔ نگهداری نمایه‌ساز، ساختمان داده‌ها و اجزای داخلی نمایه‌ساز و غیره) چگونه قلمداد می‌کنید؟	۲/۴۳	
۴-۷		میزان اهمیت ویژگی ((سرعت الگوریتم‌های جستجو)) در نمایه‌ساز:	۲/۴۳	
۴-۸		میزان اهمیت ویژگی ((اندازه نمایه‌ساز)) در نمایه‌ساز:	۲/۱۳	
۴-۹		میزان اهمیت ویژگی ((عوامل ادغام)) در نمایه‌ساز:	۱/۷۳	
۴-۱۰		میزان اهمیت ویژگی ((ساختمان‌داده نمایه‌ساز)) در نمایه‌ساز:	۲/۴	
۴-۱۱		میزان اهمیت ویژگی ((تکنیک‌های ذخیره‌سازی)) در نمایه‌ساز:	۲	
۴-۱۲		کدام‌یک از سیاست‌های دفاعی زیر در مرحلهٔ نمایه‌سازی یا رتبه‌بندی جویش‌گرهای بومی برای مقابله با وب‌سایت‌های آلوده استفاده می‌شود؟ (میزان اهمیت هر یک را با امتیاز مشخص کنید). ۱. اگر جویش‌گر بعد از خزش، یک صفحه وب را آلوده تشخیص دهد، آن صفحه را در زمان نمایه‌سازی با میزان رتبهٔ کمتری نمایه می‌کند تا کاربران با احتمال کمتری به صفحات آلوده هدایت شوند.	۱/۰۷	
۴-۱۳		۲. اگر جویش‌گر پس از خزش، یک صفحه وب را آلوده تشخیص دهد، آن صفحه را رتبه‌بندی و نمایه‌سازی نمی‌کند و به‌طور کامل آن صفحهٔ وب را از پایگاه دادهٔ خود حذف می‌کند.	۲/۹۳	
۵	مرحلهٔ رتبه‌بندی	آسیب‌پذیری وابسته به بخش مؤلّفه رتبه‌بندی		
۵-۱		میزان اهمیّت و تأثیر حملهٔ صفحات تکراری (هک پراکسی[1]) را در رتبه‌بندی جویش‌گر چگونه قلمداد می‌کنید؟	۲/۸۳	۲/۲۶
۵-۲		میزان اهمیّت و تأثیر حملهٔ محتوای تکراری (ریسندگی محتوا[2]) را در رتبه‌بندی جویش‌گر چگونه قلمداد می‌کنید؟	۲/۷	
۵-۳		میزان اهمیت و تأثیر حملات مربوط به تغییر نشانی (صفحات پنهان[3] و تغییر مسیر زیرکانه[4]) را در رتبه‌بندی جویش‌گر چگونه قلمداد می‌نمایید؟	۲/۷	
۵-۴		میزان اهمیت و تاثیر حملات مربوط به (مزارع پیوند[5]) را در رتبه‌بندی جویش‌گر چگونه قلمداد می‌کنید؟	۳/۷۴	
۵-۵		میزان اهمیت و تأثیر حملات مربوط به چاشنی واژهٔ کلیدی[6] را در رتبه‌بندی جویش‌گر چگونه قلمداد می‌کنید؟	۳/۲۳	
۵-۶		میزان اهمیت و تأثیر حملات مربوط به صفحات درگاه[7] را در رتبه‌بندی جویش‌گر چگونه قلمداد می‌کنید؟	۱/۸۷	

[1] Proxy Hacking
[2] Article Spinning
[3] Clocking Pages
[4] Sneaky Redirect
[5] Link Farms
[6] Keyword Stuffing
[7] Doorway Pages

۵-۷		میزان اهمیت و تأثیر حملات مربوط به واژگان کلیدی و پیوندهای مخفی را در کدهای تحت وب رتبه‌بندی جویش‌گر چگونه قلمداد می‌کنید؟	۲/۵۵	
۵-۸		میزان اهمیت عامل ((دامنه تارنماها)) را در رتبه‌بندی جویش‌گر چگونه ارزیابی می‌کنید؟	۱/۸۷	
۵-۹		میزان اهمیت عامل ((سرویس‌دهندهٔ تارنماها)) را در رتبه‌بندی جویش‌گر چگونه ارزیابی می‌کنید؟	۱/۸۷	
۵-۱۰		میزان اهمیت عامل ((معماری تارنماها)) را در رتبه‌بندی جویش‌گر چگونه ارزیابی می‌کنید؟	۱/۸۷	
۵-۱۱		میزان اهمیت عامل ((محتوای تارنماها)) را در رتبه‌بندی جویش‌گر چگونه ارزیابی می‌کنید؟	۳/۰۳	
۵-۱۲		میزان اهمیت عامل ((پیوندهای داخلی)) را در رتبه‌بندی جویش‌گر چگونه ارزیابی می‌کنید؟	۱/۳۶	
۵-۱۳		میزان اهمیت عامل ((پیوندهای خارجی)) را در رتبه‌بندی جویش‌گر چگونه ارزیابی می‌کنید؟	۱/۲۱	
۵-۱۴		میزان اهمیت عامل ((عوامل صفحه)) را در رتبه‌بندی جویش‌گر چگونه ارزیابی می‌کنید؟	۲/۱۲	
۵-۱۵		میزان اهمیت عامل ((برچسب‌ها)) را در رتبه‌بندی جویش‌گر چگونه ارزیابی می‌کنید؟	۱/۶۷	
۵-۱۶		میزان اهمیت عامل ((استفاده از سئوی کلاه‌سفید)) را در رتبه‌بندی جویش‌گر چگونه ارزیابی می‌کنید؟	۲/۴۳	
۵-۱۷		میزان اهمیت ارائه راهکارهای مقابله با حملات سئو را در مرحلهٔ ((رتبه‌بند)) چگونه ارزیابی می‌کنید؟	۲/۵۸	
۵-۱۸		میزان اهمیت استفاده از روش زیر را هنگام تشخیص صفحات و تارنماهای آلوده چگونه ارزیابی می‌کنید؟ ((قبل از اینکه کاربران به پیوند آلوده مراجعه کنند جویش‌گر پیغام هشدار "این سایت یا صفحه وب ممکن است برای سامانهٔ شما خطرناک باشد" را به کاربران نشان می‌دهند)).	۳/۴	
۵-۱۹		میزان اهمیت استفاده از روش زیر را هنگام تشخیص صفحات و تارنماهای آلوده چگونه ارزیابی می‌کنید؟ ((هیچ برخوردی با چنین تارنماهایی انجام نمی‌شود و بلافاصله پیوند آلوده را به کاربران نشان می‌دهند)).	۱/۴۷	
۵-۲۰		میزان اهمیت این موضوع که کاربران عادیِ جویش‌گرهای بومی می‌توانند صفحات وب‌اسپم به جویش‌گر گزارش کنند، چگونه ارزیابی می‌کنید؟	۲/۵	
۵-۲۱		تعداد و نوع مشخصه‌های به‌کاررفته در رتبه‌بندی صفحات وب، تا چه میزان در تضمین و تأمین امنیت جویش‌گرهای بومی می‌تواند مؤثر باشد؟	۲/۵۸	

در جدول (۲) ریسک‌ها، به تفکیک حوزهٔ آسیب‌پذیری و تهدیدهای مشترک شناسایی‌شده میان سامانه جویش‌گرهای بومی ارائه شده‌اند. امتیازات مندرج روبه‌روی هر یک از آسیب‌پذیری‌ها و تهدیدها، با امتیاز جمع‌آوری‌شدهٔ افراد شرکت‌کننده (خبرگان این حوزه) محاسبه شده است. نتایج جدول (۲) در حوزه‌های تهدیدهای جویش‌گرهای بومی به‌صورت زیر دسته‌بندی شده‌است که حاکی از اهمیت امنیت بخش کدنویسی است:

- سطح ریسک بخش مؤلفه نمایه‌ساز (۱.۹۸).
- سطح ریسک بخش مؤلفه رتبه‌بند (۲.۴۶).
- سطح ریسک بخش تنظیمات مدیریتی و پیکربندی (۳.۸۴).

- سطح ریسک بخش مؤلفه خزش‌گر (۴.۱۰).
- سطح ریسک بخش کدنویسی(۴.۳۴).

علاوه‌براین، آمارهای گزارش‌شده از شرکت‌های امنیتی Acunetix و مایکروسافت [۱۹،۴۷] نیز نشان‌دهندهٔ اهمیت رعایت کدنویسی و اعمال تنظیمات مدیریتی و پیکربندی امن در برنامه‌های کاربردی مطرح و مهمی مانند سامانهٔ جویش‌گرهای بومی است.

۴-۷- مرحلهٔ هفتم: تشخیص ریسک

در این مرحله هدف، محاسبهٔ ارزش و درجه‌بندی ریسک‌های شناسایی‌شده است. با این کار ریسک‌های شناسایی‌شده در محدودهٔ دامنهٔ امنیت اطّلاعات سامانه ارزش‌گذاری شده و در طبقات مختلف قرار داده‌می‌شوند. درنهایت دربارهٔ نحوهٔ برخورد با ریسک‌های هر طبقه و انتخاب راهبرد صحیح، تصمیم‌گیری می‌شود تا ریسک‌های سامانه را بتوان مدیریت کرد. به‌منظور ارزش‌گذاری و درجه‌بندی ریسک‌ها باید خروجی حاصل از گام‌های پنجم و ششم به‌عنوان ورودی گام هفتم بررسی و تحلیل شوند. در همین راستا، سطح تواتر و شدت اثر محاسبه‌شده برای هریک از ریسک‌های شناسایی‌شده در ماتریس جدول (۳) قرار داده‌می‌شوند.

(جدول-۳): ماتریس شناسایی ریسک

		میزان تاثیر		
		کم (۱۰)	متوسط (۵۰)	بالا(۱۰۰)
تواتر اتفاق	بالا (۱)	ریسک (۱*۱۰=۱۰)	ریسک (۱*۵۰=۵۰)	ریسک (۱*۱۰۰=۱۰۰)
	متوسط(۰/۵)	ریسک (۰/۵*۱۰=۵)	ریسک (۰/۵*۵۰=۲۵)	ریسک (۰/۵*۱۰۰=۵۰)
	کم (۰/۱)	ریسک (۰/۱*۱۰=۱)	ریسک (۰/۱*۵۰=۵)	ریسک (۰/۱*۱۰۰=۱۰)

با استفاده از رابطهٔ (۳) امتیاز نهایی هر ریسک را که مبین ارزش تخصیص‌یافته به آن است، می‌توان محاسبه کرد:

میزان ریسک = میزان تأثیر * تواتر اتفاق (۳)

در روش‌شناسی NIST توصیهٔ ویژه‌ای مبنی بر تعیین معیار تصمیم‌گیری و میزان درجهٔ آن نشده‌است (برخی از روش‌شناسی‌ها برای این بخش، توصیهٔ مشخصی ارائه نکرده‌اند)؛ همچنین چنانچه تعداد بسیاری از ریسک‌های شناسایی‌شده در یک طبقه قرار گرفتند که عملیات ارزش‌گذاری میان ریسک‌های یک طبقه باید دوباره انجام شود. بنابراین درصورتی‌که اقدامات درنظرگرفته‌شده برای کنترل ریسک‌های شناسایی‌شده (با توجّه به ارزش‌گذاری انجام‌شده) به اجرا گذاشته‌نشود، و گواهینامهٔ امنیت اطلاعات صادر شود، منجر به ازدست‌رفتن اعتبار گواهینامهٔ بالا خواهدشد.

۴-۸- مرحلهٔ هشتم: توصیه‌های کنترلی

در این مرحله، هدف شناسایی کنترل‌هایی‌است که برای مدیریت ریسک‌های درجه‌بندی‌شده در مرحلهٔ پیش ضروری است. کنترل‌های شناسایی‌شدهٔ این بخش باید حاصل ارزش‌گذاری ریسک، باشد؛ چراکه هر کنترل باید به یک ریسک شناسایی‌شده در سامانه مرتبط شود. ممکن است، برای کاهش یک ریسک شناسایی‌شده نیازی به اعمال کنترل نباشد یا با یک کنترل چند ریسک را بتوان مدیریت کرد.

توجه به این نکته ضروری است که برای یک ریسک ضعیف نباید از کنترل قوی استفاده کرد؛ زیرا این امر هزینه‌بر است؛ بنابراین در این مرحله، همواره باید به تحلیل هزینه[1] توجه شود. در همه بحث‌های مدیریتی این مسئله مطرح است که همیشه باید از نیازمندی‌های کسب و کار به راه‌کار رسید.

در مبحث مدیریت ریسک نیز با همین رویکرد ابتدا باید ریسک‌های موجود را شناسایی، سپس اقدام به شناسایی کنترل‌های متناظر کرد. توجه به این نکته ضروری‌ست که برای کنترل و مدیریت ریسک همواره نیاز به اعمال کنترل نیست. گاهی ریسک را به مرجع دیگری در خارج از سازمان (در صورت تأیید اعتبار) می‌توان منتقل کرد (به بخش "کاهش ریسک" در همین مقاله مراجعه شود). برای اجرای کنترل‌ها نیز راه‌های بی‌شماری وجود دارد. با وجود عدم‌ضرورت اعمال و اجرای همه ۱۳۳کنترل ذکرشده در ISO 27002، تحلیل نادرستِ هزینه و استفادهٔ نابه‌جا و نامناسب از ابزارهای کنترلی، منجر به از دست رفتن گواهینامهٔ امنیت اطلاعات می‌شود؛ همچنین، در این مرحله باید به این نکته

[1] Cost & Benefit

اشاره شود که چرا یک کنترل کنار گذاشته شده و برای حذف هرکدام نیز بهتر است، دلیل قانع‌کننده‌ای مانند هزینه وجود داشته‌باشد. در جدول (۴) کنترل‌های امنیتی پیرو نتایج حاصل‌شده از ارزیابی به‌صورت عمومی ارائه شده‌است:

(جدول-۴): کنترل‌های امنیتی توسعه سامانه جویش‌گرهای بومی (عمومی).

تهدید متناظر	کنترلی‌های امنیتی توسعهٔ سامانهٔ جویش‌گرهای بومی (عمومی)
پیکربندی نادرست امنیتی	اعمال صحیح سیاست‌های مؤلفه خزش‌گر در سامانهٔ جویش‌گرهای بومی به‌منظور بالابردن پایداری، کارایی و مقابله با دام‌های خزش‌گر؛ این سیاست‌ها با توجه به محتوا و کاربران هدف جویش‌گرها باید به‌گونه‌ای انتخاب شوند که علاوه‌بر حفظ کارایی و سودمندی جویش‌گرها، پایداری آن خدشه‌دار نشود. به‌عنوان مثال تله‌های خزش‌گر منجر به اتلاف فضای زیادی از مخزن ذخیره‌سازی شود.
پیکربندی نادرست امنیتی	درنظرگرفتن تدابیر لازم برای جلوگیری از هرزنگاری با استفاده از الگوریتم جمع‌آوری و رتبه‌بندی جویش‌گرهای بومی؛ مهاجم با استفاده از هرزنگاری می‌تواند تارنماهای مورد نظر خود را در صدر نتایج جستجوی کاربران قرار دهد. با این کار درعمل جویش‌گرها از ارائهٔ سرویس بازمانده و تبدیل به وسیلهٔ تبلیغاتی برای مهاجمان می‌شوند.
پیکربندی نادرست امنیتی، افشای اطلاعات حساس و مهم و پردازه گذاری فراوبگاهی	آگاه‌کردن و حفاظت از اطلاعات کاربر از خطرهای امنیتی موجود در نتایج جستجو با انتخاب سازوکار صحیح و دقیق توسط جویش‌گرهای بومی؛ گزارش‌های بسیاری وجود دارد که جویش‌گرها در زمان نمایش نتایج جستجو با نمایش بخشی از محتوای ناامن سایت امنیت کاربران خود را به خطر انداخته‌اند[۴۸]. این سامانه‌ها باید این‌گونه محتواها را در هنگام نمایش نتایج جستجو حذف کنند. همچنین، برخی از مهاجمان با استفاده از جویش‌گرها و کلیدواژه‌های جذاب، کاربران را به مشاهده سایت خود ترغیب می‌کنند. یکی از جدیدترین موارد مربوط به باج‌افزارهاست که با قفل‌کردن رایانهٔ شخص، وی را مجبور به پرداخت مبلغی برای برگرداندن به حالت عادی می‌کنند. و درحالی‌که کاربر برای یافتن راه حل در جویش‌گرها به جست‌وجو می‌پردازد سایت مهاجم نمایش داده‌شده و کاربر قربانی با مراجعه به آن دچار تهدید دیگری می‌شود. درنتیجه، جویش‌گرها باید خطر سایت‌های ناامن را به کاربرانی که از روی پیوند آنها کلیک می‌کنند، هشدار دهد. با این کار از حملهٔ فرد مهاجم به‌وسیلهٔ جویش‌گرها جلوگیری می‌شود.
پیکربندی نادرست امنیتی و افشای اطلاعات حساس و مهم	عدم‌وابستگی سامانهٔ جویش‌گرهای بومی به سرویس‌دهنده‌های خارج از کشور برای ارائهٔ سرویس‌ها و استفاده از سرویس‌دهنده‌های داخلی؛ با توجه به پیاده‌سازی شبکهٔ اینترانت ملی، سرویس‌دهی جویش‌گرهای بومی نباید وابسته به شبکهٔ ارتباطی خارج از شبکهٔ داخلی باشد. این خود امکان خروج ترافیک داده‌ها را از مرزهای کشور کاهش داده و منجر به افزایش امنیت داده می‌شود.
پیکربندی نادرست امنیتی	پراکندگی مؤلفه‌های سامانهٔ جویش‌گرهای بومی هنگام موازی‌سازی و تکرار در مناطق جغرافیایی مختلف؛ این عمل در کنار استقلال مؤلفه‌ها و مقاومت در برابر خرابی یک یا چندین بخش جویش‌گر نقش به‌سزایی در افزایش پایداری سامانه به‌خصوص در خسارت‌های فیزیکی دارد.
پیکربندی نادرست امنیتی	توزیع‌پذیری و تکرارپذیری در مؤلفه‌هایی مانند خزش‌گر، رتبه‌بند و سامانهٔ ذخیره‌سازی در معماری سامانه جویش‌گرهای بومی، تکرارپذیری اجزای معماری برای افزایش کارایی، جلوگیری از ا شباع شدن و افزایش پایداری سامانه است؛ همچنین با توزیع‌کردن داده‌ها در سرویس‌دهنده‌های مختلف، پایداری سامانه افزایش می‌یابد.
افشای اطلاعات حساس و مهم	رعایت مسائل مربوط به حریم شخصی کاربران در جمع‌آوری اطلاعات و ثبت تعامل کاربران با سامانه؛ در واقع سامانهٔ جویش‌گرهای بومی نباید ناقض حریم امنیتی کاربران خود باشند. این نقض حریم در تحلیل اطلاعات تعامل کاربر با سامانه یا دسته‌بندی و ارائهٔ داده می‌تواند به‌گونه‌ای باشد که حملهٔ فرد مهاجم (به‌ویژه حملات مربوط به مهندسی اجتماعی) را تسهیل کند. به‌این‌ترتیب، فرد مهاجم از این نوع سامانه برای یافتن سریع هدف خود و حمله به آن بدون ردپا استفاده می‌کند. هر سازمان توسعه‌دهنده یا ارگانی که اطلاعات خود را در وب قرار می‌دهد، باید روالی مدون برای بررسی محتوای اطلاعاتی که سازمان در اختیار عموم قرار می‌دهد، داشته، این اطلاعات را قبل از فرد مهاجم یافته و از روی وب حذف کند.
پیکربندی نادرست امنیتی	رعایت اعمال ملاحظات پدافند غیرعامل در بسترهای نرم‌افزاری نظیر پایگاه‌داده، مستندات، سیستم‌عامل و سرویس‌دهندهٔ وب؛ ازآن‌جایی‌که کارکرد سامانهٔ جویش‌گرهای بومی وابسته به سامانه‌های نرم‌افزاری، بستر سخت‌افزاری و شبکه است، عدم‌رعایت این ملاحظات، امنیت و پایداری این نوع سامانه‌ها را با خطر مواجه می‌کند.
افشای اطلاعات حساس و مهم	استفاده از سازوکارهای مناسب برای حفاظت از الگوریتم‌های به‌کاربرده‌شده و محرمانه باقی‌ماندن معماری نرم‌افزار. چراکه در اختیار داشتن و آشنایی با بخش‌های گوناگون معماری سامانه جویش‌گرهای بومی منجر به تسهیل نفوذ مهاجمان به سامانه و منع خدمت می‌شود.

پیکربندی نادرست امنیتی و افشای اطلاعات حساس و مهم	استفاده از استانداردها و پروتکل‌های امنیتی بومی به‌منظور حفظ امنیت اطلاعات تبادل‌شده بین مؤلفه‌های سامانهٔ جویش‌گرهای بومی که درغیراین‌صورت امکان شنود، تحلیل داده‌های مهم (در خدمات مهمی که این نوع سامانه‌ها ارائه می‌دهند، مانند سرویس رایانامه، شبکه‌های اجتماعی، نقشه) و ردیابی اطلاعات (ارزشمند) افراد وجود دارد.
پیکربندی نادرست امنیتی	به‌کار بردن برنامه‌های متن‌باز با استفاده از روش‌های بهینه‌سازی کد، اضافه‌کردن بسته‌ها و سرویس‌های امنیتی سخت‌افزاری و نرم‌افزاری بومی متناسب با اجزا، بستر معماری و ارتباطی.

۹-۴- مرحلهٔ نهم: مستندسازی نتایج

تمام اقداماتی که تا این مرحله انجام شده است، تنها درصورت مستندسازی، پذیرفته می‌شوند؛ همچنین مستندات باید به تأیید مراجع ذی‌صلاح در سازمان توسعه‌دهندهٔ سامانهٔ جویش‌گرهای بومی رسیده‌باشد. مراجع ذی‌صلاح در سازمان‌های مختلف با توجه به نوع فعالیت سازمان متفاوت هستند. با این حال در تمامی سازمان‌ها امضای مدیرعامل و مدیر امنیت اطلاعات همواره مهم است. خروجی مرحلهٔ نهم، شامل گزارش ارزش‌گذاری ریسک‌های شناسایی‌شده در محدودهٔ دامنه امنیت اطلاعات سازمان می‌شود که باید از موارد زیر تشکیل شده باشد:

- فهرست تهدیدهای شناسایی‌شده (مرحلهٔ سوم ارزش‌گذاری ریسک).
- فهرست آسیب‌پذیری‌های متناظر با هر تهدید (مرحلهٔ چهارم ارزش‌گذاری ریسک)
- فهرست کنترل‌های موجود با ذکر تهدید مرتبط (مرحلهٔ هشتم ارزش‌گذاری ریسک)
- شدت اثر و تواتر وقوع ریسک شناسایی‌شده برای هر تهدید (مرحلهٔ هفتم ارزش‌گذاری ریسک)
- درجهٔ ارزش هر ریسک (مرحلهٔ پنجم و ششم ارزش‌گذاری ریسک)

کنترل پیشنهادی برای مدیریت هر ریسک، ارزش‌گذاری و درجه‌بندی ریسک‌های شناسایی‌شده در محدودهٔ دامنهٔ امنیت اطلاعات برنامه‌های کاربردی سامانهٔ توسعه‌دهنده تکمیل می‌شود و به این ترتیب، نخستین مرحلهٔ مدیریت ریسک، یعنی ارزیابی ریسک به اتمام می‌رسد. مرحلهٔ دوم و سوم از مدیریت ریسک باید متناسب با نتایج به‌دست‌آمده از آزمون ارزیابی آسیب‌پذیری هریک از انواع سامانه جویش‌گرهای بومی انجام شود.

۵- نقش‌های کلیدی و عوامل موفقیت در فرآیند مدیریت ریسک

از جمله کسانی که نقش فعال در پیاده‌سازی مدیریت ریسک در سامانهٔ جویش‌گرهای بومی دارند، به افراد زیر می‌توان اشاره کرد:

- مدیر ارشد سامانهٔ توسعه‌دهنده، مدیر ارشد اطلاعاتی[1]
- صاحبان و مسئولان سامانه و اطّلاعات آن
- مدیران عملیاتی، مدیر امنیت اطّلاعات و تعلیم‌دهندگان مسائل امنیتی سامانه

علاوه‌براین، از دیگر عوامل و افرادی که در فرآیند مدیریت ریسک باید مد نظر قرار گیرند، عبارتند از:

- مشتریان
- کاربران
- تیم پروژه
- پروژه‌های مرتبط با تأمین‌کنندگان

فرایند مدیریت ریسک، فرایندی مبتنی بر ارتباط بین عوامل و افراد عنوان‌شده در بالاست و در آن فناوری اطلاعات به‌عنوان یک عامل کلیدی شناخته‌می‌شود؛ همچنین، یک برنامهٔ موفق در مدیریت ریسک فناوری اطّلاعات وابسته به عوامل زیر است:

- تعهّد مدیر ارشد در خصوص زمان و منابع پشتیبانی و همکاری همه‌جانبهٔ گروه
- صلاحیت تیم مدیریت ریسک فناوری اطلاعات
- آگاهی و مشارکت کاربران سامانه ارزیابی مستمر و شناسایی مداوم ریسک‌های مربوط به مأموریت فناوری اطلاعات

۶- نتیجه‌گیری

در این مقاله به ارزیابی و اجرای مدیریت ریسک مطابق با اطلاعاتِ جمع‌آوری‌شده بر مبنای پرسش‌نامهٔ طراحی‌شده، برای شناسایی ریسک‌های مهم سامانهٔ جویش‌گرهای بومی با استفاده از روش‌شناسی NIST پرداخته شده‌است. نتایج حاصل از این پژوهش به‌منظور افزایش سطح امنیت انواع

[1] Chief Information Officer(CIO)

سامانهٔ جویش‌گرهای بومی آینده در اختیار مدیران پروژه، توسعه‌دهندگان، طراحان و سایر ذی‌نفعان می‌تواند قرار گیرد.

نگاشت انجام‌شده میان تهدیدها و آسیب‌پذیری‌ها (مطابق جدول (۱)) براساس شماره‌های شناسه‌های تعیین‌شده از سوی مؤسسه‌های امنیتی، بیان‌گر وابستگی و ارتباط میان آن‌هاست؛ به‌گونه‌ای که این موضوع در مدیریت و انتخاب روش صحیح مقابله با ریسک می‌تواند تأثیرگذار باشد؛ ازاین‌رو، برای شناسایی مهم‌ترین تهدیدها و آسیب‌پذیری‌ها در سامانهٔ جویش‌گرهای بومی به‌ترتیب از رویکرد STRIDE به‌کمک ابزار Microsoft Threat Modeling و آزمون جعبهٔ سیاه استفاده شد. سطح ریسک به‌دست‌آمده، به تفکیک انواع حوزه‌های تهدید شناسایی‌شده، نشان‌دهندهٔ اهمیت رعایت کدنویسی امن در توسعهٔ این نوع برنامه‌های کاربردی تحت وب است؛ همچنین، از میان مؤلفه‌های به‌کاررفته در سامانهٔ جویش‌گرهای بومی (خزش‌گر، رتبه‌بند و نمایه‌ساز) بالاترین سطح ریسک محاسبه‌شده، به مؤلفهٔ خزش‌گر تعلّق دارد. حال به‌منظور مقابله و برخورد با ریسک‌های شناسایی‌شدهٔ متناسب با این نوع برنامهٔ کاربردی تحت وب، استفاده از رویکرد کاهش و پذیرش ریسک مانع سوءاستفاده از آسیب‌پذیری‌ها و تهدیدها مهم و می‌تواند جدی شود. به این منظور مطابق جدول (۶) نمونه توصیه‌های کنترلی عمومی آورده شده‌است.

تشکّر و قدردانی

این پژوهش با حمایت پژوهشکدهٔ امنیت مرکز تحقیقات مخابرات ایران انجام شده‌است و در این راستا از این مرکز، همچنین از جناب آقای مهندس خالقی‌دخت، (سرپرست پژوهشکدهٔ امنیت) و راهنمایی‌های سرکار خانم دکتر نادری (مجری پروژهٔ نقشهٔ راه امن‌سازی سامانهٔ جویش‌گرهای بومی) تشکّر و قدردانی می‌شود.

۷- مراجع

[1] J. a. C. S. Zimmermann, in *"Handbook on Project Management and Scheduling Vol. 2."*, 2015.

[2] P. e. a. Cichonski, in *"Special Publication 800-61 Revision 2." Computer Security Incident Handling Guide.*, NIST, 2012.

[3] R. a. A. J. Ross, in *"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach." NIST Special Publication 800-37.*, NIST, 2010.

[4] R. Lepofsky, The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web,, Apress, 2014.

[5] Risk Management Guide for Information Technology System, Special Publication 800-30,p. 1., National Institute of Standards and Technology, July,2002.

[6] "Bannerman, Paul L," in *"Risk and risk management in software projects: A reassessment." Journal of Systems and Software 81.12*, 2008, pp. 2118-2133.

[7] ش .نادری، ن .تاج نیشابوری، ا .صلاحی، ف .احمدپناه، و ح .کوشککی" نام گزارش :چرخه حیات امن سیستم پروژه: نقشه راه امن سازی جویش‌گر بومی، "مرکز تحقیقات مخابرات ایران، تهران، 1394/12/25 .

[7] Sh.Naderi, N. Taj Neyshaburi, E.Salahi, F Ahmadpanah, and h. koshkaki "Report Name: Secure Life Cycle of the Project System: Securing Local Search Engine Road Map, Tehran Telecommunication Research Center, Tehran, 2015.

[8] S. Elky, An introduction to information systems risk management, 2006.

[9] S. Radack, The system development life cycle (sdlc), Computer Security Division Information Technology Laboratory National Institute of Standards and Technology., 2002.

[10] ز .ب .ع .محمد ,"طراحی و پیاده‌سازی سامانه‌های خزش و رتبه‌بندی اسناد فارسی وب و پیاده‌سازی یک جویش‌گر فارسی"، ایران، تهران :پ مرکز تحقیقات مخابرات ایران، تهران، 1391/11/21.

[10] Z. B. E Mohammad, "Design and Implement Crawling and Ranking Systems of Persian Documents in the Web and Implementing a Persian Search Engine", Iran, Tehran Telecommunication Research Center, Tehran, 2012.

[11] ح .کوشککی، و ش .نادری"امنیت در مؤلفه‌ها و معماری جویش‌گرها، "کنفرانس بین المللی مهندسی کامپیوتر و فناوری اطلاعات دانشگاه تهران، تهران 1395/03/12.

[11] h. Koshkaki, and Sh. Naderi "Security in the Components and Architecture of Search Engines," International Conference on Computer Engineering and Information Tech-nology, University of Tehran, Tehran, 2015.

[12] T. OWASP, ""Top 10–2013." The Ten Most Critical Web Application Security Risks," 2013.

[13] P. L. M. M. G. F. Matteo Meucci, in *OWASP Testing Guide v4*, The OWASP Fundation, 2015.

[14] Acunetix, "Acunetix Web Application Vulnerability Report," 2016.

[15] P. Bowen, Information Security Handbook: A Guide for Managers (NIST Special Publication 800-100). Gaithersburg, MD: Computer Security Division.", Information Technology Laboratory, National Institute of Standards and Technology, 2006.

[16] B. Potter, "Microsoft SDL threat modelling tool.," Elsevier, 2009.

[17] A. Shostack, in *Threat modeling: Designing for security*, John Wiley & Sons, 2014.

[18] R. K. W. a. W. J. Scandariato, ""A descriptive study of Microsoft's threat modeling technique." Requirements Engineering 20.2," 2015, pp. 163-180.

[19] م .امیدوار سرکندی، ش .نادری، و ف .ا .احمدپناه"ارائه یک مدل نوین برای ایمن‌سازی جویش‌گرهای بومی با رویکرد دفاع در عمق، "تهران، دانشگاه صنعتی امیرکبیر، 1395/02/24.

[19] M. Omidvar Sarkandi, Sh. Naderi and F. Ahmadpanah "A New Model to Secure Search Engines based on Defence in Depth Approach", Tehran, Amirkabir University of Technology, 2015.

[20] Q. Huang, ""Research on Risk Analysis and Management in the Software Development Process.","2015 5th International Conference on Education, Management, Information and Medicine (EMIM 2015), 2015.

[21] Calder, Alan, and Steve Watkins. IT governance: A manager's guide to data security and ISO 27001/ISO 27002. Kogan Page Ltd., 2008.

[22] ISO/IEC. "ISO/IEC 27002: 2005 information technology-security techniques–code of practice for information security management." (2005).

[23] International Organization for Standardization, and International Electrotechnical Commission. Information Technology: Secur-ity Techniques: Code of Practice for Information Security Management. ISO/IEC, 2005.

[24] "Codex," [Online]. Available: http://codedx.com/security-misconfiguration/.

[25] "htbridge," [Online]. Available: https://www.htbridge.com/vulnerability/insufficient-session-expiration.html.

[26] "CAPEC-60," [Online]. Available: http://capec.mitre.org/data/definitions/60.html.

[27] "CAPEC-10," [Online]. Available: http://capec.mitre.org/data/definitions/10.html.

[28] "CAPEC-100," [Online]. Available: http://capec.mitre.org/data/definitions/100.html.

[29] "CAPEC-134," [Online]. Available: https://cwe.mitre.org/data/definitions/134.html.

[30] "CAPEC-311," [Online]. Available: https://cwe.mitre.org/data/definitions/311.html.

[31] "CAPEC-444," [Online]. Available: https://cwe.mitre.org/data/definitions/444.html.

[32] "CAPEC-63," [Online]. Available: https://capec.mitre.org/data/definitions/63.html.

[33] "CAPEC-16," [Online]. Available: https://capec.mitre.org/data/definitions/16.html.

[34] [Online]. Available: h-ttps://capec.mitre.org/data/definitions/15.html.

[35] "CAPEC-400," [Online]. Available: https://cwe.mitre.org/data/definitions/400.html.

[36] "CAPEC-345," [Online]. Available: https://cwe.mitre.org/data/definitions/345.html.

[37] "CAPEC-148," [Online]. Available: https://capec.mitre.org/data/definitions/148.html.

[38] "CAPEC-93," [Online]. Available: https://cwe.mitre.org/data/definitions/93.html.

[39] "CAPEC-105," [Online]. Available: https://capec.mitre.org/data/definitions/105.html.

[40] "CAPEC-34," [Online]. Available: https://capec.mitre.org/data/definitions/34.html.

[41] "CAPEC-273," [Online]. Available: https://capec.mitre.org/data/definitions/273.html.

[42] "Checkupdown," [Online]. Available: http://www.checkupdown.com/status/E502.htl.

[43] "webappsec," [Online]. Available: http://www.webappsec.org/.

[44] "SANS," [Online]. Available: h-ttps://www.sans.org/.

[45] "mapping," [Online]. Available: 7. Http://www.criticalwatch.com/assets/c-Owasp-to-Wasc-to-CWE-Mapping-Tech-Paper-0710131.pdf.

[46] A. M. B. W. M. C. J.D. Meier, "Cheat Sheet: Web Application Security Frame," May 2005. [Online]. Available: h-ttps://msdn.microsoft.com/en-us/library/ms978518.aspx

[47] A.Charlie, D.Kaufman, A.Penta ,Microsoft Security Intelligence Report Volume 20 July through December, 2015.

[48] Edelman, Benjamin. Assessing and Improving the Safety of Internet Search Engines, 2007.

مهسا امیدوار سرکندی مدرک کارشناسی خود را در رشته مهندسی کامپیوتر گرایش نرم‌افزار در سال ۱۳۹۳ از دانشگاه آزاد اسلامی، واحد تهران–جنوب دریافت کرد. وی هم‌اکنون دانشجوی رشتهٔ کارشناسی ارشد نرم‌افزار دانشگاه صنعتی امیرکبیر است. زمینه‌های پژوهشی مورد علاقهٔ ایشان امنیت نرم‌افزار، ارزیابی آسیب‌پذیری و تهدیدهای برنامه‌های کاربردی، تحلیل و طراحی نرم‌افزارهای امن و پایگاه‌های تحت ابر است.

نسرین تاج فارغ التحصیل کارشناسی ارشد مهندسی فناوری اطّلاعات، گرایش مخابرات امن در سال ۸۸ از دانشگاه علم و صنعت ایران و پژوهش‌گر مرکز تحقیقات مخابرات ایران است. زمینه‌های پژوهشی ایشان امنیت شبکه و فناوری اطّلاعات، امنیت جویش‌گر بومی و مدیریت فناوری اطلاعات است و تاکنون بیش از ده‌ها مقاله در مجلات علمی-پژوهشی وکنفرانس‌های داخلی و خارجی به چاپ رسانیده‌است.

شقایق نادری کارشناسی خود را در مهندسی کامپیوتر از دانشگاه خوارزمی دریافت کرد. تحصیلات کارشناسی ارشد و دکتری خود را در رشته مهندسی کامپیوتر گرایش نرم‌افزار از دانشگاه تربیت مدرس به‌ترتیب در سال‌های ۱۳۸۱ و ۱۳۹۱ به پایان رسانده‌است. وی درحال حاضر استادیار پژوهشگاه ارتباطات و فناوری اطلاعات است. زمینه‌های پژوهشی مورد علاقهٔ ایشان یادگیری ماشین و پردازش تصویر است.

حسن کوشککی مدرک کارشناسی خود را در رشته مهندسی فناوری اطلاعات در سال ۱۳۹۱ از دانشگاه پیام نور و مدرک کارشناسی ارشد خود را در رشته مهندسی فناوری اطلاعات-امنیت اطلاعات در سال ۱۳۹۴ از دانشگاه تربیت مدرس دریافت کرد. زمینه‌های پژوهشی مورد علاقه ایشان امنیت شبکه و اطلاعات، شبکه‌های کامپیوتری، امنیت مالتی‌مدیا، جریان‌سازی مدیا روی اینترنت، جریان‌سازی ویدیوی نظیر به نظیر، امنیت سامانه‌های مبتنی بر شهرت و طراحی امن معماری شبکه است.