

ارائه شاخص‌های امنیتی در چرخه حیات توسعه سامانه جویس گر بومی

نسرین تاج نیشابوری^{۱*}، شقایق نادری^۲، مهسا امیدوار سرکندی^۳ و حسن کوشکی^۴

۱ کارشناس ارشد امنیت مرکز تحقیقات مخابرات، پژوهشکده امنیت، تهران، ایران
n_taj@itrc.ac.ir

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

۳ پژوهشگر امنیت مرکز تحقیقات مخابرات، پژوهشکده امنیت، تهران، ایران
m.omidvarsarkandi@itrc.ac.ir
hassan.kooshkaki@gmail.com

چکیده

حفظ اعتبار نزد کاربران و ذی‌نفعان و ارائه خدمات مهم و متنوع با حفظ ویژگی دسترسی پذیری بالا، در جویس‌گرهای بومی قابل تأمل و بررسی است؛ از این رو معرفی و نحوه به‌کارگیری ابزارهای کنترل امنیتی در مؤلفه‌ها و اجزای اصلی جویس‌گرهای بومی مانند خزش‌گر، رتبه‌بند و نمایه‌ساز، به‌همراه ملاحظات امنیتی سرویس‌های تحت وب جویس‌گر در تمامی مراحل چرخه حیات توسعه جویس‌گرهای بومی، اصلی‌ترین محور این مقاله را تشکیل می‌دهد. این مقاله سعی دارد با بررسی استانداردهای امنیتی مرتبط با چرخه حیات توسعه جویس‌گرهای بومی و با در نظر گرفتن اجزای تشکیل‌دهنده کلیدی جویس‌گرهای بومی، نحوه ترکیب تمامی این ابعاد را در چرخه حیات توسعه جویس‌گرهای بومی معرفی کرده تا طراحان، با اعمال صحیح و به‌موقع ملاحظات و کنترل‌های امنیتی، بتوانند به بهره‌برداری ایمن و با کیفیتی از مؤلفه‌ها و اجزای اصلی جویس‌گرهای بومی دست یابند.

واژگان کلیدی: جویس‌گرهای بومی، چرخه حیات امن توسعه سامانه، ملاحظات امنیتی، کنترل امنیتی، مؤلفه‌ها و شاخص‌های امنیتی در چرخه حیات توسعه سامانه جویس‌گر

۱- مقدمه

امروزه چالش امنیت در دسترسی به اطلاعات، جدی‌تر از فقدان اطلاعات است. با توجه به اهمیت پیاده‌سازی امنیت در چرخه حیات توسعه سامانه و همچنین با توجه به آمارهای مشاهده‌شده [1]، بارز است که شرکت‌های خارجی، آشنایی اندکی با روش‌های ایمن‌سازی چرخه حیات توسعه سامانه‌ها دارند. محور اصلی این مقاله معرفی ابزارهای کنترل امنیتی در مؤلفه‌ها و اجزای اصلی جویس‌گرهای بومی مانند خزش‌گر، رتبه‌بند، نمایه‌ساز و ملاحظات امنیتی در سرویس‌های تحت وب در جویس‌گرهای بومی در تمامی مراحل چرخه حیات توسعه جویس‌گرهای بومی است. این مقاله با بررسی

استانداردهای امنیتی مرتبط با چرخه حیات یک سامانه و مطالعه دقیق اجزا، چگونگی ترکیب تمامی این ابعاد و ملاحظات امنیتی را در دوره حیات توسعه آن‌ها معرفی کرده تا متولیان جویس‌گرهای بومی با رعایت و اعمال این موارد، بتوانند بهره‌برداری امن و با کیفیتی از مؤلفه‌ها و اجزای اصلی جویس‌گرهای بومی ارائه کنند [2]، [3].

۲- نحوه اعمال ابزارهای کنترلی در امن‌سازی سرویس‌های جویس‌گرهای بومی

* نویسنده عهده‌دار مکاتبات

قابلیت‌های پیچیده‌تر با یکدیگر می‌توانند ترکیب شوند و محل ارائه آن‌ها بر روی اینترنت، اینترنت یا ماشین‌های محلی و حتی به صورت ترکیبی از همه این موارد باشد. اما چگونه یک سرویس را می‌توان امن ساخت؟ کلید امن‌سازی سرویس‌های یک سامانه شامل شناسایی، تشخیص و مدل‌سازی است که توضیح آن به اجمال، به شرح زیر است:

- شناسایی اهداف امنیتی و نیازمندی‌های امنیتی سامانه. این مهم با شناسایی تهدیدها و آسیب‌پذیری‌های یک سامانه امکان‌پذیر است.
- تشخیص اینکه این تهدید مربوط به زمان حال یا آینده است بر اساس تهدیدهای شناخته‌شده صورت می‌گیرد.
- همچنین مدل‌سازی تهدید یک روش مؤثر برای کمک به شناسایی تهدیدها و آسیب‌پذیری‌های مربوطه و اولویت‌بندی آن‌ها است. همچنین با این روش، توسعه‌دهندگان می‌توانند آسیب‌پذیری‌ها را آزمایش و بررسی کنند.

سرویس‌های اصلی ارائه‌شده در جویس‌گرهای بومی مبتنی بر وب هستند. لحاظ کردن امنیت در طول چرخه حیات توسعه سامانه از ابزار اصلی ایجاد امنیت در جویس‌گرهای بومی است؛ زیرا در طی این عمل با استفاده از مدل تهدیدها طراحی بخش‌های مختلف مانند کد، استقرار و آزمایش را می‌توان بهبود بخشید [5].

۱-۲- بررسی چرخه حیات توسعه امن در جویس‌گرهای بومی

بر طبق بررسی‌های به‌عمل‌آمده، هر محصول، سامانه، خدمت، صنعت یا کسب و کاری دارای یک دوره عمر است. بدین معنی که در یک مقطعی از زمان، متولد و معرفی می‌شود، رشد می‌کند، به مرحله بلوغ و سپس مرحله اشباع و در آخر زوال آن فرا می‌رسد؛ لذا باید به‌گونه‌ای برنامه‌ریزی کرد که همواره خروجی مورد انتظار در مرحله رشد و بلوغ خود باقی بماند؛ چون پس از آن در صورت هدایت و برنامه‌ریزی ناصحیح دوران بی‌حاصلی آن پدیدار شده و در نهایت منجر به نابودی آن خواهد شد. با توجه به مفهوم کلی بالا، می‌توان گفت تئوری چرخه عمر در مواردی همچون محصولات، سامانه‌ها، بازار، خدمات، فناوری و صنعت و حتی امنیت نیز کاربرد دارد و لذا از طریق تعیین جایگاه هر یک از عوامل بالا در طول چرخه تصویری واضح

برقراری امنیت و تداوم آن در این سامانه‌ها یکی از مهمترین چالش‌های عصر کنونی است که دست‌یابی به آن در گرو موارد زیر امکان‌پذیر است:

- شناسایی اصول و ابزارهای کنترل امنیتی و چارچوب‌ها و الگوهای امنیتی؛
- لحاظ کردن امنیت در مراحل دوره حیات سامانه و ارزیابی شاخص‌های امنیتی درگیر در هر یک از آن‌ها [18].

واژه کنترل به معنای تنظیم یک ابزار، سازوکار یا رویه است که به‌کارگیری آن موجب کاهش مخاطرات در یک سامانه می‌شود. به عبارت دیگر برای کاهش مخاطرات حاصل از هر تهدید، لازم است از یک یا چند ابزار کنترلی استفاده شود؛ همچنین ممکن است یک کنترل ساده یا مرکب به‌منظور کاهش مخاطره ناشی از چند تهدید هم‌زمان، به‌کارگرفته شود. کنترل‌ها ممکن است از نوع فنی، عملیاتی یا مدیریتی باشند که با دید ملاحظات امنیتی ترکیب می‌شوند. برخی از ابزارهای کنترل امنیتی در دسته فنی شامل مواردی چون دیوار آتش، رمزکننده و نرم‌افزار آنتی‌ویروس هستند. از نمونه کنترل‌های امنیتی عملیاتی به رویه‌های تهیه نسخه پشتیبان، پاسخ‌گویی به انواع حوادث امنیتی و برگزاری آزمایشگاه‌های آزمایش می‌توان اشاره و در زمینه کنترل‌های امنیتی مدیریتی از طرح امن‌سازی کسب و کار و سیاست‌های امنیتی در تداوم کسب و کار می‌توان استفاده کرد [2]، [3]. قبل از بررسی سرویس‌های امنیتی مورد نیاز در جویس‌گرهای بومی لازم است به اجمال به مفهوم امن‌سازی در سرویس‌ها بپردازیم. امنیت به‌طوراساسی در مورد حفاظت از دارایی‌های یک سامانه یا سازمان شکل می‌گیرد. دارایی‌ها ممکن است موارد ملموس، مانند عملیات و یا پایگاه داده‌های یک سامانه و یا به‌طورکامل ناملموس، مانند شهرت و اعتبار اجرایی یک سامانه یا سازمان باشد. در هنگام امن‌سازی یک سامانه باید زیرساخت و برنامه‌های کاربردی را تجزیه و تحلیل و تهدیدات بالقوه را شناسایی کرد. درحقیقت امنیت همان مدیریت ریسک و اجرای اقدامات متقابل و مؤثر است و امنیت مؤثر ترکیبی از مردم، فرآیند، و فناوری است. امنیت متکی بر ارکان: احراز هویت، مجازشماری، حسابرسی و انکارناپذیری، محرمانه‌بودن، تمامیت و یکپارچگی و دردسترس‌بودن است؛ اما تعریف کلی سرویس چیست؟ سرویس می‌تواند یک رابط عمومی باشد که دسترسی به یک واحد عملیاتی را فراهم کند. سرویس‌ها جهت ارائه

سامانه‌ای واحد، سرویس دست‌یابی به فناوری اطلاعات را ارائه می‌دهند. به بیان دیگر جویس‌گرهای بومی، یک سامانه اطلاعاتی تحت وب هستند که هدف اصلی آن هدایت کاربران در دستیابی بهتر به اطلاعات مورد نیاز است؛ لذا با لحاظ کردن این دستورالعمل در جویس‌گرهای بومی ضمن مشخص کردن نقش‌های کلیدی امنیت و مسئولیت‌هایی که در توسعه بیش‌تر سامانه‌های اطلاعاتی مورد نیاز است و با افزودن فعالیت‌های امنیتی درون روش‌شناسی SDLC به امنیت چرخه حیات توسعه سامانه می‌توان دست یافت. مدیریت مناسب ریسک‌های جویس‌گرهای بومی بر پایه محرمانگی، یکپارچگی و دسترس‌پذیری، همچنین الحاق این ملاحظات امنیتی منجر به افزودن سناریوهای توسعه مانند معماری سرویس‌گرا و مجازی‌سازی به چرخه توسعه سامانه خواهد شد و توسعه سنتی سامانه را متحول خواهد کرد؛ حتی سازمان‌ها خواهند توانست این توانمندی را در چرخه توسعه خود از راه‌های زیر اعمال کنند:

- تشخیص سریع و به‌موقع آسیب‌پذیری‌های امنیتی، پیگیربندی نامناسب و پیاده‌سازی کنترل امنیت با قیمت کمتر و کاهش آسیب‌پذیری‌ها؛
 - افزایش کنترل امنیتی با آگاهی از چالش‌های مهندسی؛
 - مشخص کردن سرویس‌های امنیتی به‌اشتراک گذاشته‌شده که منجر به کاهش هزینه توسعه و استفاده مجدد از راهبردها و ابزارهای امنیتی می‌شود؛
 - اتخاذ تصمیم‌گیری آگاهانه هنگام مدیریت ریسک‌ها در زمان لازم؛
 - مستندسازی تصمیمات امنیتی مهم از طریق توسعه و اجرای مدیریت مطمئن ریسک‌ها در تمام مراحل؛
 - افزایش اعتماد مشتری و سازمان در جهت ترویج سرمایه‌گذاری؛
 - جلوگیری از اختلالات بعدی با افزایش ایمنی در تعاملات بین سامانه‌ای.
- همان‌طور که گفته شد، استاندارد NIST SP 800-64 با رویکرد ریسک‌محور بر روی امنیت در سامانه‌های اطلاعاتی متمرکز شده است. این بدان معنی است که با ایجاد امنیت در این سامانه‌ها، خروجی‌های ارزشمندی از نظر مشخص کردن ریسک‌ها و کاهش آن‌ها پدید می‌آید که

و دقیق نسبت به اقدامات و تمهیداتی که باید در آینده صورت گیرد، می‌توان به‌دست آورد. در این ارتباط مطالعه رفتار و عملکرد محصولات و سامانه‌ها در طول دوره عمرشان نیز قابل توجه است. برای مثال ضرایب شدت و تکرار حوادث و یا میزان پاسخ‌های پیش‌بینی‌شده همواره یکسان نبوده و بسته به هر مرحله از دوره عمر متفاوت هستند. هر دوره عمر برای دوام و تعالی خود نیاز به توجه کافی به ابعاد امنیتی خود دارد؛ به‌عبارتی امن کردن چرخه‌های حیات از مهم‌ترین ابعاد لازم در این کار است. گاهی نیز چرخه حیات‌ها چنان در هم ادغام می‌شوند که برای یک محصول، سامانه یا سازمان به‌صورت ترکیبی استفاده می‌شوند؛ به‌عنوان مثال امنیت چرخه حیات توسعه سامانه با امنیت چرخه حیات توسعه نرم‌افزار که با توجه به اجزای تشکیل‌دهنده جویس‌گرهای بومی، می‌توان گفت امنیت چرخه حیات توسعه سامانه و امنیت چرخه حیات توسعه نرم‌افزار در حفظ و ابقای سامانه‌های جویس‌گرهای بومی با توجه به ماهیت تکوین و خروجی‌های مورد انتظار آن به‌شدت با یکدیگر درگیر می‌شوند. استاندارد NIST SP 800-64 چارچوب مدیریت ریسک را با نقشه راه ساده‌ای برای تجمیع توابع امنیتی در داخل چرخه حیات توسعه سامانه^۱ کامل می‌کند. این ملاحظات امنیتی برای هر مرحله آورده شده است؛ لذا کاربردهای کسب و کار و نیازمندی‌های امنیتی به‌طور هم‌زمان در طی چرخه توسعه حیات جویس‌گرهای بومی، پیشرفت داده می‌شود تا توازن و تعادل میان این دو برقرار شود [4].

۲-۲- بررسی استاندارد (NIST SP 800-64)

این استاندارد [4] درخصوص امنیت در چرخه حیات توسعه سامانه/ سازمان و یک راهبرد جامع برای مدیریت کردن ریسک‌های مربوط به دارایی‌های فناوری اطلاعات در یک سازمان است؛ که با ادغام فعالیت‌های امنیتی ضروری در داخل چرخه حیات توسعه سامانه، صورت می‌پذیرد. در نتیجه این عمل هزینه‌ها را می‌تواند کاهش دهد و کنترل امنیتی مناسبی روی ریسک‌ها، فرآیند توسعه و آزمایش اعمال کند؛ اما قبل از هرچیز باید تعریف دقیقی از جویس‌گرهای بومی ارائه کرد تا جایگاه آن‌ها در هنگام بررسی این استاندارد، مشخص شود. جویس‌گرهای بومی ترکیبی از سخت‌افزارها و نرم‌افزارهایی است که تحت

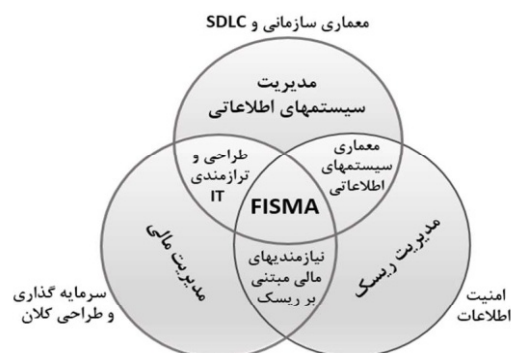
¹ SDLC(Secure Development Life Cycle)

• انجام BIA³ یا تجزیه تحلیل تاثیر کسب و کار و ارتباط آن با کارایی سامانه جهت مشخص سازی ارتباط سامانه و دارایی ها با سرویس های حساس و بررسی پیامدهای ناشی از اختلال آن ها؛

مدیریت ریسک و مدیریت منابع مالی نیز در بخش نیازمندی های مالی مبتنی بر ریسک با یکدیگر مشترکند. در دیدگاه مدیریت ریسک در استاندارد NIST SP 800-39 با رویکرد سامانه ای/ سازمانی به تشریح یک چارچوب از مدیریت ریسک های امنیتی در سامانه های اطلاعاتی پرداخته شده است. همچنین این استاندارد به دنبال برقراری تعادل در حفاظت از دارایی ها و اطلاعات سامانه/ سازمان با راهبرد کنترل هزینه و کاهش ریسک در طی چرخه حیات توسعه سامانه است. در خصوص این استاندارد در بخش های بعدی توضیح داده خواهد شد. در بخش تداخل حوزه مدیریت فناوری اطلاعات و مدیریت منابع مالی باید دانست که مؤثرترین راه برای پیاده سازی مدیریت ریسک، مشخص کردن عملیات و دارایی های حساس و آسیب پذیری های نظام مند است. ریسک ها مشترک هستند و توسط سازمان، منابع درآمد یا توپولوژی سازمان محدود نمی شوند. مشخص کردن عملیات و اصلاح منابع حساس و ارتباطات بین این دو از طریق فرآیند طراحی امنیت سامانه و تدوین اطلاعات حاصل می شود. دو فرایند CPIC به معنی برنامه ریزی و کنترل سرمایه گذاری و EA به معنای معماری سازمانی در ایجاد این دیدگاه در عملیات مهم تجاری یک سازمان دخیلند. آن ها از دارایی های یک سامانه یا سازمان پشتیبانی کرده و وابستگی ها و ارتباطات را به وجود می آورند. با مشخص کردن عملیات و دارایی های حساس، سازمان ها می توانند یک BIA یا تجزیه تحلیل تاثیر کسب و کار انجام دهند. هدف از BIA ارتباط سامانه و دارایی ها با سرویس های حساس و بررسی پیامدهای ناشی از اختلال آن ها است. براین اساس در یک سامانه/ سازمان تأثیرات امنیت را بر روی اولویت ها می توان مدیریت کرد. این کار برای آسان کردن برنامه هایی در خصوص کارایی هزینه، تأثیرات تجارت و ارزش آن برای سازمان یا سامانه است. با دیدگاه مدیریت ریسک در یک سامانه یا یک پروژه، امنیت از همان ابتدا در سرتاسر سامانه و چرخه حیات CPIC وجود دارد. با این کار نقش برجسته ای از اندازه گیری و تحمیل نیازمندی های امنیتی در سرتاسر مرحله های چرخه حیات مستند خواهد شد. مدیران از این اطلاعات در

در جهت مدیریت و توسعه فناوری اطلاعات از آن استفاده می شود. براین اساس حوزه های مدیریت سامانه های اطلاعاتی، مدیریت ریسک و مدیریت منابع مالی در انجام این فعالیت به صورت سه گانه با یکدیگر درگیر می شوند که این تداخل در شکل (۱) نشان داده شده است:

در بخش مدیریت سامانه های اطلاعاتی، معماری و چرخه حیات توسعه سامانه (SDLC) شکل می گیرد و در تداخل با حوزه مدیریت ریسک، وارد بخش معماری سامانه های اطلاعاتی و چارچوب FISMA می شود. همچنین در تداخل با حوزه مدیریت مالی، وارد بخش طراحی و ترازمندی پروژه های فناوری اطلاعات شده و دوباره از چارچوب FISMA استفاده می شود.



(شکل-۱) ترکیب حوزه های مدیریتی با سیستم های اطلاعاتی [4]

- این چارچوب وجه مشترک هر سه حوزه مدیریت است. براساس الگوی این استاندارد، یک سامانه اطلاعاتی با دو حوزه مدیریت ریسک و مدیریت منابع مالی درگیر است و برای برقراری امنیت آن در چرخه حیات توسعه سامانه نکات زیر بایستی لحاظ شود:
- مشخص شدن معماری سازمانی (EA¹).
- مشخص کردن معماری سامانه ای؛ با استفاده از مدیریت ریسک و چارچوب FISMA؛
- بودجه بندی و طراحی بخش های مختلف یک سامانه براساس مدیریت منابع مالی و انجام CPIC²؛
- مشخص کردن عملیات و دارایی های حساس و آسیب پذیری های سامانه جهت الویت بندی های مالی و بالابردن آمادگی ریسک پذیری آن؛

³ Business Impact Analysis

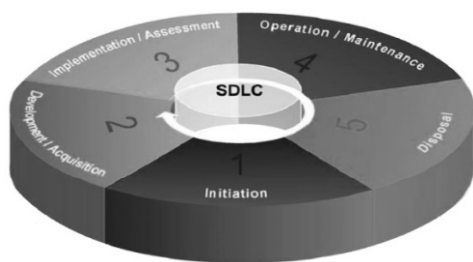
¹ Enterprise Architecture

² Capital Planning and Investment Control

استاندارد NIST SP 800-53,39 با توجه به حفظ محرمانگی، یکپارچگی و دسترس‌پذیری سامانه‌های اطلاعاتی امکان‌پذیر خواهد بود. با استناد به این استاندارد، جویس‌گرهای بومی باید معماری جامع امنیتی، ابزار، تخصص‌ها و نیازهای کسب و کار و سرویس‌های امنیتی لازم حین کار خود را پیش‌بینی کرده و طرح پیاده‌سازی منطبق با فرهنگ و راهبردهای سازمانی که جویس‌گرهای بومی را پشتیبانی و تغذیه می‌کند. آشکار شود. به‌طور معمول این معماری با انجام زمان‌بندی مناسبی از وظایف، فعالیت‌های مورد انتظار، تخمین منابع مورد نیاز جویس‌گرهای بومی و وابستگی‌های کلیدی آن، تکمیل می‌شود [5]، [6].

۳- چگونگی ترکیب امنیت با چرخه حیات توسعه سامانه

استاندارد NIST SP 800-64 چارچوب مدیریت ریسک را با نقشه راه ساده‌ای برای تجمیع توابع امنیتی در داخل SDLC کامل می‌کند. این ملاحظات امنیتی برای هر مرحله از SDLC آورده شده است؛ لذا کاربردهای کسب و کار و نیازمندی‌های امنیتی به‌طور همزمان در طی چرخه توسعه پیشرفت داده می‌شود تا توازن و تعادل بین این دو برقرار شود. شکل (۳) یک دیدگاه مفهومی از مراحل این چرخه حیات است:



(شکل-۲): نگاه مفهومی به مراحل چرخه حیات توسعه سامانه [4]

۳-۱- مرحله نخست چرخه حیات توسعه سامانه و ملاحظات امنیتی وابسته به آن

همان‌طور که در شکل (۳) دیده می‌شود، ملاحظات امنیت در مرحله نخست یا همان مرحله شروع SDLC درجهت استحکام صحت اطلاعات است و لذا باید در این مرحله این اطمینان حاصل شود که تهدیدها، نیازمندی‌ها و محدودیت‌ها در عملکرد سامانه مورد توجه کافی قرار

خودپیداآوری و چرایی تصمیمات گرفته‌شده و ارزیابی بیشتر آن می‌تواند استفاده کنند. همچنین گروه‌های حساس‌تری و نظارت نیز از این اطلاعات در بازنگری برای اصلاح مدیریت سیستم و مشخص کردن نقاطی که امنیت در آن نقاط نادیده گرفته شده می‌تواند استفاده کنند؛ همچنین می‌تواند امتحان کنند که آیا این مستندات به درستی نشان می‌دهند که سامانه حقیقتاً چگونه اجرا و نگهداری می‌شود؟ مدل ساده و معمول SDLC شامل پنج مرحله زیر است:

- شروع: در طی این مرحله نیاز به یک سامانه و هدف آن مستند می‌شود؛
 - توسعه/ اکتساب: در این مرحله سامانه طراحی، خریداری، برنامه‌ریزی و توسعه‌یافته و ساخته می‌شود.
 - ارزیابی/ پیاده‌سازی: پس از آزمایش موفقیت‌آمیز سامانه، نصب آن انجام می‌شود؛
 - نگهداری/ اجرا: در طی این مرحله سامانه کار تعیین‌شده را انجام داده، مورد بهره‌برداری قرار می‌گیرد و توسط افزودن سخت‌افزار و نرم‌افزار و حوادث دیگر اصلاح می‌شود؛
 - امحا: فعالیت‌های انجام‌شده در طی این مرحله اطمینان می‌دهد که سامانه به‌طور منظم خاتمه یافته و امحا می‌شود، حفظ اطلاعات حیاتی سامانه و انتقال داده‌های پردازش‌شده توسط سامانه به سامانه جدید و حفظ آن مطابق سیاست‌ها و قوانین مدیریتی قابل اجرا از وظایف این مرحله است. در هر یک از این مراحل دست‌کم نیازمندی‌های امنیتی در فرایندهای توسعه سامانه لحاظ شده است. همچنین در چرخه حیات سامانه، موارد زیر بر اساس مأموریت سازمان، معماری سامانه یا سازمان و فرآیندهای مالی بررسی می‌شود:
 - دیدگاهی به فعالیت‌های اساسی و نقاط تحویل مرحله؛
 - دروازه‌های کنترلی و نقاط تصمیم‌گیری؛
 - خروجی‌های ویژه و ورود اطلاعات حیاتی در طراحی سامانه؛
 - انجام و نگهداری سامانه- امنیت و ملاحظات اجرایی توسعه سامانه.
- همچنین چرخه حیات توسعه یک سامانه باید از معماری امنیتی برخوردار باشد که این مهم براساس

بدون معماری کسب و کار انجام نمی‌پذیرد؛ لذا طبقه‌بندی امنیت در آغاز چرخه حیات سامانه جویس‌گرهای بومی منجر به تشکیل بهتر EA و CPIC می‌شود، که همان‌طور که در قسمت‌های قبل گفته شد، به‌منظور مشخص شدن معماری داخلی جویس‌گرهای بومی و تأمین منابع مالی آن مورد نیاز خواهد بود.

۲-۳- مرحله دوم چرخه حیات توسعه سامانه و ملاحظات امنیتی وابسته به آن

فعالیت‌های امنیتی افزوده‌شده به مرحله توسعه/ اکتساب شامل:

- ارزیابی ریسک‌ها و استفاده از این نتایج به‌عنوان مکملی برای کنترل امنیتی پایه در جویس‌گرهای بومی؛
- تحلیل نیازمندی‌های امنیتی جهت برطرف کردن گپ‌ها یا افزودنی‌های بلااستفاده در جویس‌گرهای بومی؛
- انجام توابع و آزمایش‌های امنیتی جویس‌گرهای بومی به‌منظور امکان اعمال بازخورد و برگشت به مراحل قبل؛
- آماده کردن مستندات اولیه برای تأیید و گواهی‌بخشیدن به سامانه جویس‌گرهای بومی؛
- طراحی معماری امنیتی به‌صورت گرافیکی و با جزئیات به‌نحوی که مکان و چگونگی کنترل‌های امنیتی در آن نشان داده شود. خلاصه این معماری و راهبردهای لحاظ‌شده در طراحی امنیتی سامانه جویس‌گرهای بومی آورده شده است. این بخش اجزای امنیت اطلاعات را در یک نگاه ترتیبی از بالا به پایین قرار می‌دهد؛ ولی این اجزا لزوماً ثابت نیستند. از تحلیل امنیتی یک سامانه پیچیده باید به‌طور ثابت بازخورد گرفته تا به‌تدریج کامل شود. مستندات امنیتی در جویس‌گرهای بومی باید با موارد زیر تراز شود:
- تحلیل نیازمندی‌های امنیتی [7] جویس‌گرهای بومی
- معماری امنیتی جویس‌گرهای بومی؛
- ارزیابی تأثیرات کسب و کار و طبقه‌بندی امنیتی اطلاعات در جویس‌گرهای بومی.

گرفته‌اند. امنیت در این نقطه مطابق ریسک‌های کسب و کار، اطلاعات اداره امنیت اطلاعات مشخص شده‌اند. به‌عنوان مثال، نتایج ریسک سیاسی از یک وب‌گاه مهم که در یک دوره تجاری خاص، دست‌کاری شده یا در دسترس نبوده، سبب کاهش اعتماد شهروندان خواهد شد. فعالیت‌های امنیتی در مرحله شروع شامل:

- نیازمندی‌های کسب و کار سازمان توسعه‌دهنده جویس‌گرهای بومی از نظر محرمانگی، صحت و دسترس‌پذیری تشریح شود که خروجی آن آموزش امنیتی تیم توسعه‌دهنده و طرح‌های تضمین کیفیت در سامانه و استانداردهای کدنویسی و توسعه سامانه جویس‌گرهای بومی خواهد بود. همچنین راهبردهای کسب و کار مشخص می‌شوند. باید اطمینان حاصل کرد که ذی‌نفعان درگیر در سامانه خدمات جویس‌گرهای بومی درک مشترکی از میزان پیچیدگی سامانه و نیازمندی‌ها و ملاحظات امنیتی آن دارند. قوانین و تنظیمات و استانداردهای مربوطه در کار مشخص شود. نقش‌های امنیتی در توسعه سامانه لحاظ شود. این قسمت زمان زیادی خواهد گرفت؛ چون افراد باید براساس توانایی‌های خود مسئولیت پذیر باشند؛
 - طبقه‌بندی اطلاعات از نظر امنیتی در مخازن جویس‌گرهای بومی و مشخصه‌هایی که برای انتقال و ذخیره‌سازی اطلاعات به‌کار گرفته می‌شود، نظیر شناسه‌های شخصی که خروجی آن مشخص شدن نیازمندی‌های امنیتی سطح بالا و تخمین سطح تأثیر آن‌ها خواهد بود؛
 - مشخص کردن تمامی نیازمندی‌های حریم خصوصی در جویس‌گرهای بومی.
- نتیجه یک طراحی آگاهانه و به‌موقع، صرفه‌جویی در وقت و هزینه و طراحی مناسب در مدیریت ریسک جویس‌گرهای بومی است. مباحث امنیتی به‌عنوان بخشی از توسعه سامانه باید به‌کار گرفته شوند (نه به‌صورت مجزا). کارکنان یک سازمان یا کاربران جویس‌گرهای بومی باید بدانند که برخورد مقطعی از طبقه‌بندی امنیت و تحلیل تأثیرات کسب و کار¹ (BIA) در انجام هر فعالیتی باید مدنظر قرار گیرد. هیچ سرمایه‌گذاری در فناوری اطلاعات

¹ Business Impact Analysis

۳-۳- مرحله سوم چرخه حیات توسعه

سامانه و ملاحظات امنیتی وابسته به آن

در طی مرحله سوم سامانه در محیط اجرایی یک سازمان، نصب و ارزیابی می‌شود. فعالیت‌های امنیتی لازم در مرحله ارزیابی / پیاده‌سازی شامل موارد زیر است:

- ارائه جزئیات طراحی برای C&A^۱؛
- یک پارچگی‌سازی امنیت در داخل محیط یا سامانه مربوطه که خروجی آن اصلاح فهرست کنترل‌های امنیتی اجرایی جویس‌گرهای بومی است.
- تأمین امنیت سامانه دسترسی که خروجی آن گزارش ارزیابی امنیتی جویس‌گرهای بومی و بسته احراز اصالت امنیتی و ورودی برای POA&M^۲ است.
- الزام استفاده از سامانه اطلاعات احراز اصالت به‌منظور تصمیم‌گیری‌های امنیتی در جویس‌گرهای بومی؛
- هماهنگی کامل میان طراحی و انجام فعالیت‌های گواهی و تأیید سامانه با آزمایش کنترل امنیت جویس‌گرهای بومی که خروجی آن بازنگری مالی، به‌روزرسانی آن، بررسی آمادگی توسعه سامانه جویس‌گرهای بومی و تصویب اتصالات موجود آن است.

۳-۴- مرحله چهارم چرخه حیات توسعه

سامانه و ملاحظات امنیتی وابسته به آن

در مرحله نگهداری / اجرا، سامانه در مرحله‌ای است که در حال اصلاح و بهبود، توسعه و آزمایش است و سخت‌افزارها و نرم‌افزارها، در حال افزوده‌شدن یا جایگزینی هستند. در این مرحله جویس‌گرهای بومی نیز باید براساس نیازهای امنیتی مورد بررسی قرار گیرد تا به عملکرد مفید خود ادامه دهد. سامانه عملیاتی شده به‌طور مرتب در حال بازبینی به‌منظور اطمینان حاصل‌کردن از عملکردشان با توجه به نحوه پاسخ‌دهی به نیازهای یک سازمان در مرحله نگهداری و به‌هنگام خطرهای توافق‌شده کارتر و امن‌تر هستند. فقط در صورت اصلاح و تغییرات این مرحله، جویس‌گرهای بومی به مرحله می‌توانند بروند. بنابراین فعالیت‌های پیوستی امنیتی در این مرحله شامل: بررسی آمادگی اجرایی برای توسعه جویس‌گرهای بومی.

- مدیریت پیکربندی جویس‌گرهای بومی که خروجی آن کنترل تغییرات، به‌روزرسانی اسناد امنیتی و ارزیابی امنیتی.
- نگهداری پیوسته فرایندها و توابع سازمانی برای اجرای مطمئن کنترل‌های امنیتی سامانه اطلاعاتی جویس‌گرهای بومی که خروجی آن انجام احراز اصالت‌های مورد نیاز در جویس‌گرهای بومی خواهد بود.

۳-۵- مرحله پنجم چرخه حیات توسعه

سامانه و ملاحظات امنیتی وابسته به آن

مرحله آخر توسعه جویس‌گرهای بومی در معرض استفاده قرارگرفتن محصول است. در مرحله پنجم امحا هنگام انتقال در سامانه‌های اطلاعاتی باید از حفاظت منابع دولتی و دارایی‌های آن اطمینان حاصل کرد. به‌طورمعمول هیچ نقطه مشخصی به‌عنوان پایان یک سامانه وجود ندارد. هر سامانه‌ای به‌دلیل پیشرفت فناوری و تغییر نیازمندی‌ها ناگزیر است که به سمت نسل بعدی خود در حال حرکت باشد. لذا طراحی امنیت جویس‌گرهای بومی باید به‌طور مداوم همراه با سامانه در حال رشد کردن باشد. بیش‌تر اطلاعات اجرایی مدیریتی و محیطی وابسته به طراحی امنیتی سامانه‌های تابعه است. خاتمه سامانه باید به‌طور منظم با حفظ و ذخیره اطلاعات حیاتی نظیر طراحی‌های امنیتی و نیازمندی‌های کنترل امنیت باشد تا در صورت نیاز مجدد، برخی یا همه اطلاعات گذشته قابل فعال‌سازی باشند. بنابراین تأکید ویژه‌ای بر روی حفاظت از داده‌های پردازش‌شده یک سامانه در ضمن انتقال به سامانه دیگر یا هنگام بایگانی وجود دارد. این ذخیره‌سازی باید براساس سیاست‌ها و تنظیمات مدیریتی ثبت کاربردی اطلاعات جهت دسترسی‌های آینده و یا به‌روزرسانی‌های بعدی باشد. فعالیت‌های امنیتی در این مرحله:

- ساختن و اجرای طرح واگذاری / انتقال محصول جویس‌گرهای بومی
- بایگانی اطلاعات حیاتی سامانه جویس‌گرهای بومی
- حفاظت از اسناد و مدارک حیاتی در محیط یا رسانه و طبقه‌بندی آن که منجر به مشخص کردن سطح ریسک‌های سامانه جویس‌گرهای بومی می‌شود.

¹ Certification and accreditation

² Plan of Action and Milestone

همچنین بر مبنای کنترل‌های امنیتی و خروجی های مورد انتظار در هر مرحله، شاخص‌های امنیتی اصلی در هر مرحله از چرخه حیات را در هر یک از اجزا و ساختار معماری جویس‌گرهای بومی و سرویس‌های تحت وب به بحث گذاشتیم. در نهایت جدول سه‌بعدی که متشکل از اجزای اصلی جویس‌گرهای بومی، سرویس‌های تحت وب مرتبط با آن، مؤلفه‌های امنیتی و شاخص‌های ارزیابی امنیتی در هر یک از مراحل چرخه حیات توسعه امن سامانه با ملاحظات چرخه حیات نرم‌افزاری، حاصل شد؛ که نمونه‌ای از ارزیابی امنیتی از نوع تشخیص در سطح فنی جویس‌گرهای بومی می‌تواند باشد. [17]، [16] نتیجه پژوهش‌ها و مطالعات بالا در قالب جدول (۱) آورده شده است.

در اختیار گذاشتن رکوردهای ثبت موجودی‌های سخت‌افزاری و نرم‌افزاری جویس‌گرهای بومی (خریداری شده، اهدایی یا کنار گذاشته شده) و به‌روزرسانی فهرست موجودی‌ها بر اساس نیازهای امنیتی یا به‌کارگیری در پروژه‌های دیگر یا از بین بردن آن در صورت عدم نیاز و وجود اطلاعات خطرناک.

۴- استخراج شاخص‌های امنیتی در چرخه حیات امن جویس‌گرهای بومی

بر اساس مطالعات انجام‌شده [15]-[8]، موفق به استخراج مؤلفه‌های امنیتی بیشتر و دقیق‌تری نسبت به دیگر مؤلفه‌های امنیتی حائز اهمیت در هر مرحله از چرخه حیات توسعه امن سامانه جویس‌گرهای بومی شدیم.

(جدول-۱): شاخص‌های امنیتی در چرخه حیات امن جویس‌گرهای بومی

مؤلفه‌های امنیتی مورد تأکید		فعالیت‌های امنیتی در چرخه حیات توسعه سامانه		
مرحله ۱- شروع		خرش‌گر- نمایه‌ساز-رتبه‌بند	سرویس‌های تحت وب	
Robust.Trust.CIA	1. Initiate Security Planning	زمانبندی فعالیت‌های امنیتی از نظر تقدم و تاخر	<p>در توسعه یک سرویس به‌دلیل ماژولار کردن بخش‌ها باید فعالیت‌ها و سیاست‌های امنیتی در هر کدام از بخش‌ها به‌صورت مجزا اعمال شود؛ به‌طوری که در هر بخش مسائل امنیتی با درجه اهمیت بالاتر باید زودتر پیاده‌سازی شوند. زمان‌بندی فعالیت‌های امنیتی به‌صورت سلسله‌مراتبی برای سه مؤلفه اصلی جویس‌گر به‌شرح زیر است:</p> <p>خرش‌گر:</p> <ul style="list-style-type: none"> توسعه الگوریتم‌های خرش‌گر و سیاست‌های امنیتی موجود در آن‌ها پیاده‌سازی فاکتورهای طراحی نرم‌افزاری و ساختارافزای خرش‌گر پیاده‌سازی پایگاه داده خرش‌گر <p>نمایه‌ساز:</p> <ul style="list-style-type: none"> توسعه الگوریتم‌های نمایه‌سازی و سیاست‌های امنیتی موجود در آن‌ها پیاده‌سازی فاکتورهای طراحی نرم‌افزاری و ساختارافزای نمایه‌ساز پیاده‌سازی پایگاه داده نمایه‌ساز <p>رتبه‌بند:</p> <ul style="list-style-type: none"> توسعه الگوریتم‌های رتبه‌بندی و سیاست‌های امنیتی موجود در آن‌ها 	<p>در توسعه یک سرویس به‌دلیل ماژولار کردن بخش‌ها باید فعالیت‌ها و سیاست‌های امنیتی در هر کدام از بخش‌ها به‌صورت مجزا اعمال شود؛ به‌طوری که در هر بخش مسائل امنیتی با درجه اهمیت بالاتر باید در اولویت قرار گیرد. زمان‌بندی فعالیت‌های امنیتی سرویس به‌شرح زیر است:</p> <ul style="list-style-type: none"> مروری بر مفاهیم اصلی امنیت در چرخه حیات سرویس‌های تحت وب تهیه مقدمه‌ای از طراحی امنیتی، مدل‌سازی تهدید، کدنویسی امن، آزمایش امنیتی و موارد مربوط به حریم خصوصی توجه به استانداردها، منابع، موارد مربوط به امنیت سرویس‌های تحت وب، توسعه‌دهنده و تست‌کننده و مدیر برنامه انتخاب الگوریتم‌ها و سیاست‌های امنیتی مناسب پیاده‌سازی فاکتورهای طراحی امن نرم‌افزاری و ساختارافزای انتخاب رویکردها و روش‌های امن در پایگاه داده شناسایی و ارزیابی ریسک‌های مهم

	<p>2. Categorize the Information System</p>	<p>طبقه بندی اجزاء سیستم از نظر اهمیت امنیتی روی CIA (کم، متوسط، زیاد)</p>	<p>میزان اهمیت امنیتی مؤلفه‌ها بر اساس CIA به ترتیب زیر است: نمایه‌ساز:</p> <ul style="list-style-type: none"> • پایگاه داده نمایه‌ساز بر اساس CIA بیشترین اهمیت را دارد (زیاد) • ماژول جستجو یا موتور بازیابی از لحاظ اهمیت در جایگاه دوم قرار می‌گیرد (متوسط) • الگوریتم‌ها، سیاست‌های امنیتی، ساختمان داده‌ها و نرم‌افزارهای نمایه‌سازی در جایگاه بعدی قرار می‌گیرند (متوسط) <p>خزش‌گر:</p> <ul style="list-style-type: none"> • پایگاه داده خزش‌گر نیز نسبت به اجزای دیگر خزش‌گر اهمیت بالاتری دارد (زیاد) • الگوریتم‌ها، سیاست‌های امنیتی و نرم‌افزارهای خزش‌گر در رتبه بعدی قرار می‌گیرند (متوسط) <p>رتبه‌بند:</p> <ul style="list-style-type: none"> • الگوریتم‌ها، سیاست‌های امنیتی و نرم‌افزارهای رتبه‌بندی صفحات، بالاترین اهمیت را در این مؤلفه دارند (زیاد) 	<p>میزان اهمیت امنیتی مؤلفه‌ها بر اساس CIA¹ به ترتیب زیر است: سرویس:</p> <ul style="list-style-type: none"> • پایگاه داده سرویس بر اساس CIA بیشترین اهمیت را دارد (زیاد). • ماژول جستجو (به‌عنوان مثال، در سرویس شبکه اجتماعی جستجوی افراد با ماژول جستجو انجام می‌شود) از لحاظ اهمیت در جایگاه دوم قرار می‌گیرد (متوسط). • الگوریتم‌ها، سیاست‌های امنیتی، ساختمان داده‌ها و نرم‌افزارها در جایگاه بعدی قرار می‌گیرند (متوسط). • در وب‌سرور نیز بر اساس نوع و میزان خدمت‌دهی باید ویژگی دسترسی‌پذیری را تأمین و تضمین کند (بالا). • همچنین هنگام استفاده از سرور برنامه کاربردی باید ویژگی دسترسی‌پذیری نسبت به سایر روش‌ها تأمین شود (متوسط).
	<p>3. Assess Business Impact</p>	<p>کدام بخش از سرویس در حفظ پایداری، دسترسی‌پذیری و شهرت سیستم سرویس از اهمیت بیشتری برخوردار است؟</p>	<p>نمایه‌ساز، مهم‌ترین ماژولی است که باعث پایداری و دسترسی‌پذیری جویس‌گر می‌شود؛ زیرا اگر خزش‌گر یا رتبه‌بند از کار بیفتند ولی نمایه‌ساز فعال باشد، قابلیت پاسخ به درخواست‌های کاربران بر اساس اطلاعات قدیمی وجود دارد؛</p> <p>اصلی‌ترین مؤلفه برای شهرت و محبوبیت یک جویس‌گر مؤلفه رتبه‌بند است. درواقع اگر تمام صفحات وب خزش و به بهترین نحو ممکن نمایه‌سازی شوند، اما به‌درستی رتبه‌بندی نشوند، پاسخ به پرس‌وجوهای کاربران بر اساس اطلاعات نامرتب انجام خواهد شد؛</p> <p>خزش‌گر نیز برای مسئله تازگی اطلاعات و پوشش وب اهمیت بالایی دارد. درواقع اگر پاسخ به پرس‌وجوهای کاربران بر اساس اطلاعات قدیمی صورت گیرد، نتایج نامرتب و کمتری برای نمایش وجود خواهد داشت.</p> <p>مشخص کردن اهمیت این سه مؤلفه برای دسترسی‌پذیری، پایداری و شهرت به تفکیک مشکل است؛ چون هر کدام از این مؤلفه‌ها روی یکدیگر تأثیر دارند؛ اما حالت کلی اهمیت مؤلفه‌ها به شرح زیر است.</p> <p>میزان اهمیت برای دسترسی‌پذیری و پایداری: نمایه‌ساز ← رتبه‌بند ← خزش‌گر</p> <p>میزان اهمیت برای شهرت و محبوبیت: رتبه‌بند ← خزش‌گر ← نمایه‌ساز</p> <p>رتبه‌بند ← نمایه‌ساز ← خزش‌گر</p>	<ul style="list-style-type: none"> • حفظ امنیت و ذخیره‌سازی اطلاعات تمامی کاربرانی که از سرویس‌های مهمی مانند شبکه اجتماعی، رایانامه و حساب کاربری به‌منظور شخصی‌سازی استفاده از سرویس‌ها در نظر گرفته شده، در پایگاه داده‌های مجزای هر سرویس؛ • سرویس‌های مهمی مانند شبکه اجتماعی، رایانامه و حساب‌های کاربری ویژه جهت شخصی‌سازی استفاده از سایر سرویس‌ها، از حیث حفظ حریم خصوصی کاربران، جزء مهم‌ترین سرویس‌ها به‌شمار می‌روند.

¹ Confidentiality-Integrity-Availability

	4. Assess Privacy Impact	<p>از آنجا که هسته اصلی جویش گر با اطلاعات وبسایتها در ارتباط است و ارتباط کمتری با اطلاعات کاربران دارد، درجه اهمیت حریم خصوصی کاربران کمتر است. البته اگر سرویسهای جویش گر به گونه ای باشد که کاربران اطلاعات خود را ثبت کنند انگاه باید به مسئله حریم خصوصی و امن کردن اطلاعات کاربران توجه جدی شود. به هر حال برای امن کردن و جلوگیری از نشت هر اطلاعاتی، نحوه ذخیره سازی اطلاعات در پایگاه داده باید بر اساس سیاست ها و قابلیت های زیر انجام شود:</p> <ul style="list-style-type: none"> • رمزگذاری فایل های داده برای برقراری محرمانگی داده ها؛ • ردگیری عامل انجام عملیات در پایگاه داده (نظارت پذیری)؛ • اعتبارسنجی اندازه، قالب، بازه و نوع داده های ورودی؛ • استفاده از پایگاه داده های NoSQL و چهارچوب های مدیریت محتوای توزیع شده مثل هدوپ؛ • بررسی هویت کاربران در ارتباط با ردگیری نظارتی و اجازه دسترسی به داده های خاص؛ • توجه به مسائل سازگاری اطلاعات ذخیره شده در پایگاه داده؛ • پشتیبان گیری از داده ها و اطلاعات ذخیره شده برای افزایش دسترسی پذیری؛ • گسسته سازی و دانه بندی کردن منابع ذخیره سازی؛ • امن کردن ارتباطات با استفاده از پروتکل های امنیتی بین پایگاه داده و ماژول های دیگر؛ • مدیریت قوی کلیدهای پایگاه داده ای؛ • انتخاب پایگاه داده متناسب با ابعاد و نوع داده های ذخیره شده هر سرویس. 	<p>چون برخی از سرویس های مهم جویش گر مانند شبکه های اجتماعی، رایانامه و حساب کاربری ویژه با اطلاعات کاربران در ارتباط است، درجه اهمیت حریم خصوصی کاربران و حفظ اطلاعات شخصی آنها افزایش می یابد. نحوه ذخیره سازی و نگهداری اطلاعات در پایگاه داده همواره مهم است که باید از سیاست های زیر در ذخیره سازی و نگهداری امن و اطمینان دادن به کاربر برای حفاظت اطلاعات بهره برد:</p> <ul style="list-style-type: none"> • رمزگذاری فایل های داده برای برقراری محرمانگی داده ها؛ • ردگیری عامل انجام عملیات در پایگاه داده (نظارت پذیری)؛ • اعتبارسنجی اندازه، قالب، بازه و نوع داده های ورودی؛ • بررسی هویت کاربران در ارتباط با ردگیری نظارتی و اجازه دسترسی به داده های خاص؛ • توجه به مسائل سازگاری اطلاعات ذخیره شده در پایگاه داده؛ • پشتیبان گیری از داده ها و اطلاعات ذخیره شده برای افزایش دسترسی پذیری؛ • گسسته سازی و دانه بندی کردن منابع ذخیره سازی؛ • امن کردن ارتباطات با استفاده از پروتکل های امنیتی بین پایگاه داده و ماژول های دیگر؛ • مدیریت قوی کلیدهای پایگاه داده ای؛ • انتخاب پایگاه داده متناسب با ابعاد و نوع داده های ذخیره شده هر سرویس.
	5. Ensure Secure Information System Development	<p>مشخص کردن نخستین سطح دفاع و فرصت بازیابی امنیتی</p> <p>نخستین سطوح امنیتی برای مقابله با هر گونه تهدیدی، سطح واسط کاربری و خزش گر است. زیرا این دو سطح جزء نخستین روزهایی هستند که مهاجم از طریق آنها به هسته اصلی جویش گر دسترسی می تواند پیدا کند.</p>	<p>نخستین سطوح امنیتی برای مقابله با هر گونه تهدیدی، سطح واسط کاربری و سرویس های طراحی شده است؛ زیرا این دو سطح جزء نخستین روزهایی هستند که مهاجم از طریق آنها به هسته سرویس دسترسی می تواند پیدا کند. البته در این بخش، به سرورهای مهمی همانند وب سرور نیز می توان اشاره کرد.</p>

¹ Hardware Security Module

مرحله ۲- توسعه و اکتساب			خزش‌گر- نمایه‌ساز-رتبه‌بند	سرویس‌های تحت وب
Accessibility.Integrity	1. Assess Risk to System	شناخت نقاط ضعف در طراحی ، محدودیت‌های پروژه و تهدیدها	<p>مسلماً معماری جویس‌گر باید به‌صورت دوره‌ای بررسی شود تا متناسب با تهدیدات جدید افزونه‌های امنیتی به معماری اضافه شود. مهم‌ترین تهدیدهایی که هسته اصلی جویس‌گر را هدف قرار می‌دهد آسیب‌پذیری‌های تحت وب، پایگاه داده‌ای و حمله بهینه‌سازی جویس‌گر (SEO) است که باید به‌طور پیوسته راه‌کارهای امنیتی برای آن‌ها بررسی شوند.</p>	<p>معماری سرویس باید به‌صورت دوره‌ای بررسی شود تا متناسب با تهدیدات جدید افزونه‌های امنیتی به معماری اضافه شود. همچنین باید مدل‌سازی تهدید در این مرحله صورت گیرد.</p>
	2. Select and Document Security Controls	تعیین کنترل‌های امنیتی و دسته‌بندی آن‌ها از نظر پایه‌بودن، اضافه و مکمل و سفارشی بودن. این کنترل‌های امنیتی چرا، چگونه و چگونه باید اعمال شوند؟	<ul style="list-style-type: none"> • بهره‌گیری از الگوهای برتر برای کنترل‌های امنیتی؛ • کنترل‌های امنیتی برای سیاست‌های خزش، وب‌گاه‌های آلوده و حمله بهینه‌سازی جویس‌گر (SEO) • کنترل‌های امنیتی در هنگام نمایه‌سازی برای وب‌گاه‌های آلوده و حمله بهینه‌سازی جویس‌گر (SEO) • کنترل‌های امنیتی در سطح رتبه‌بند برای مقابله با وب‌گاه‌های آلوده و حمله بهینه‌سازی جویس‌گر (SEO) • اعمال سیاست‌ها و کنترل‌های امنیتی در سطح خزش‌گر، نمایه‌ساز و رتبه‌بند به‌صورت دوره‌ای 	<ul style="list-style-type: none"> • بهره‌گیری از الگوهای برتر برای کنترل‌های امنیتی؛ • کنترل‌های امنیتی برای سیاست‌های امنیتی جستجو در وب، وب‌گاه‌های آلوده؛ • کنترل‌های امنیتی در سطح پایگاه داده برای مقابله با حملات مرتبط با آن؛ • کنترل‌های امنیتی در سطح وب‌سرور برای مقابله با حملات مرتبط با آن؛ • کنترل‌های امنیتی در سطح سرور برنامه کاربردی برای مقابله با حملات مرتبط با آن؛ • اعمال سیاست‌ها و کنترل‌های امنیتی متناسب با سرویس‌های طراحی شده.

¹ Search Engine Optimization

	<p>3. Design Security Architecture</p>	<p>معماری امنیتی مشخص شود و ابزارهای کنترلی امنیتی پایه مشخص شود.</p>	<p>برای امن کردن معماری جویس گر باید مازول های آن در ساختار امنیتی DMZ قرار گیرد تا سیاست های امنیتی مثل کنترل دسترسی، محرمانگی، صحت داده و غیره به صورت سلسله مراتبی در آن اعمال شود.</p> <p>مهم ترین ابزارهای کنترلی امنیتی پایه که روی مازول های جویس گر باید پیاده سازی شود، بدین شرح است:</p> <ul style="list-style-type: none"> • استفاده از فایروال (& EdgCast Firewall-DOM، WAF، IDS، AC و غیره برای سطوح مراحل واکنشی، نمایه سازی و جستجو؛ • امن کردن پایگاه داده ها در سطح خزش گر و نمایه ساز با استفاده از سیاست های مطرح شده در مرحله راه اندازی؛ • امن کردن ارتباطات بین سه مازول خزش گر، نمایه ساز و رتبه بند با استفاده از پروتکل های امنیتی؛ • محدود ساختن هر مازول یا کاربر به داده هایی که مجاز به دسترسی یا تغییر آن ها است؛ • پیاده سازی سیاست های کنترلی برای مبارزه با حمله بهینه سازی جویس گر (SEO) و وب گاه های آلوده در سطح رتبه بند؛ • فعال کردن سامانه ثبت وقایع به صورت گسترده برای فرایند لاگ گیری و جمع آوری فعالیت های مشکوک. 	<p>برای امن کردن معماری سرویس باید مازول های آن در ساختار امنیتی DMZ¹ و در میان حفاظ های داخلی و خارجی قرار گیرد تا سیاست های امنیتی مثل کنترل دسترسی، محرمانگی، صحت داده و غیره به صورت سلسله مراتبی در آن اعمال شود. همچنین استفاده از رویکرد دفاع در عمق به منظور افزایش امنیت در بستر سرویس های جویس گر توصیه می شود.</p> <p>مهم ترین ابزارهای کنترلی امنیتی پایه که روی مازول های سرویس باید پیاده سازی شود، بدین شرح است:</p> <ul style="list-style-type: none"> • استفاده از فایروال؛ • بررسی نوع رمزنگاری در سرویس هایی با ارزش اطلاعاتی بالا؛ • ارزیابی ضمانت امنیتی سرویس؛ • مستندسازی؛ • ارزیابی موارد پایه طراحی؛ • در نظر گرفتن حریم خصوصی در طراحی سرویس؛ • تهیه راهنمای حریم خصوصی در طراحی سرویس؛ • امن کردن پایگاه داده سرویس با استفاده از سیاست های مطرح شده در مرحله راه اندازی؛ • امن کردن ارتباطات بین اجزای سرویس؛ • محدود ساختن کاربر به داده هایی که مجاز به دسترسی یا تغییر آن ها است؛ • پیاده سازی سیاست های کنترلی؛ • فعال سازی سامانه ثبت رویداد به صورت گسترده و جمع آوری فعالیت های مشکوک.
--	--	---	---	--

¹ Demilitarized Military Zone

	<p>4. Engineer in Security and Develop Controls</p>	<p>ابزارهای کنترلی اضافی و سفارشی شده باید مشخص شوند، پیمان‌های کسب و کار و فناوری مشخص شوند، پتانسیل جهت تست آسیب پذیری‌ها یا محدودیت‌های شناخته شده فراهم گردد.</p>	<p>برای امن کردن معماری جویس‌گر و سه ماژول اصلی آن، علاوه بر کنترل‌های امنیتی پایه راه‌کارهای زیر را برای بهبود امنیت معماری می‌توان استفاده کرد:</p> <ul style="list-style-type: none"> • استفاده از ساختارهای امن SOC¹ و NOC² برای نظارت و کنترل بیشتر ماژول‌های جویس‌گر (HP Arc Sight)؛ • پیاده‌سازی سروورهای خزش‌گر، نمایه‌ساز و رتبه‌بند روی سخت‌افزارهای مجزا و ایزوله یا روی فناوری‌های مجازی Multi-Tenant ایمن • استفاده از سیاست‌های امنیتی برای مبارزه با حمله پهنه‌سازی جویس‌گر (SEO) و وب‌گاه‌های آلوده در سطح خزش‌گر و نمایه‌ساز • استفاده از ساختارهای امنیتی مثل هانی پات‌ها برای به‌دست‌آوردن اطلاعات بیشتر از مهاجمان و ارائه سناریوهای ازپیش‌تعیین‌شده به مهاجم 	<p>برای امن کردن معماری سرویس، علاوه بر کنترل‌های امنیتی پایه می‌توان راه‌کارهای زیر را برای بهبود امنیت معماری استفاده کرد:</p> <ul style="list-style-type: none"> • استفاده از ساختارهای امن برای نظارت و کنترل بیشتر اجزای سرویس • استفاده از سیاست‌های امنیتی • استفاده از ساختارهای امنیتی برای به‌دست‌آوردن اطلاعات بیشتر از مهاجمان
	<p>5. Develop Security Documentation</p>	<p>ارزیابی اثرات حریم خصوصی با توجه به بلوغ سرویس‌های امنیتی، تکمیل طرح امنیتی</p>	<p>از آنجا که جویس‌گر بیشتر با اطلاعات وب‌گاه‌ها در ارتباط هستند و فقط در زمان استفاده از سرویس‌های خاص ممکن است بر اساس اطلاعات کاربران جستجوها انجام شود. در این زمان نیاز است که سیاست‌های جلوگیری از نشت اطلاعات در جویس‌گر لحاظ شود که تا در زمان جستجوی وب‌گاه‌ها ردپای از کاربران به جای نماند. علاوه بر رعایت حریم خصوصی کاربران در زمان جستجو، جویس‌گر باید سیاست‌های امنیتی داشته باشد که از اطلاعات ذخیره‌شده کاربران در پایگاه داده نیز محافظت کند؛ این سیاست‌ها در قسمت Assess Privacy Impact از مرحله یک چرخه حیات تشریح شده است.</p> <p>علاوه بر حریم خصوصی کاربران، جویس‌گرها باید حریم خصوصی وب‌گاه‌ها را نیز در نظر بگیرند. زیرا اگر یک جویس‌گر از سیاست‌های حفظ حریم خصوصی بهره نبرد، ممکن است، اطلاعاتی از وب‌گاه را در نتایج جستجو نشان دهد که مالک وب‌گاه راضی به نشان‌دادن آن به‌طور موقت نیست. بنابراین اعمال سیاست‌های امنیتی در سطح جویس‌گر برای نقض حریم خصوصی وب‌گاه‌ها نیاز است.</p>	<ul style="list-style-type: none"> • استفاده از ساختار و تنظیمات حریم خصوصی • برای پیش‌گیری از آسیب‌های تحت سرویس؛ • به‌روزرسانی، مرور و تکمیل سند حریم خصوصی کاربران در ضمن انتشار نسخه جدید سرویس جدید و قدیم جویس‌گر

¹ Security Operation Center
² Network Operation Center

	<p>6. Conduct Developmental, Functional, and Security Testing</p>	<p>آزمون سامانه از نظر امنیت توسعه و عملکرد، ثبت تغییرات ایجاد شده غیر منتظره</p>	<p>این بخش از فاز توسعه برای هر سه مؤلفه خزش گر، نمایه ساز و رتبه بند همواره نیاز است و باید پس از توسعه نهایی مؤلفه ها آزمون های زیر انجام شود. همچنین اگر پروژه وارد دور جدید چرخه حیات شود باید سه مؤلفه مورد نظر در برابر تهدیدهای جدید بررسی و آزمایش شوند (آزمایش جعبه سفید).</p> <p>آزمون خزش گر:</p> <ul style="list-style-type: none"> • آزمایش حملات جلوگیری از سرویس؛ • آزمایش حملات تزریق کد به اسپایدرها؛ • سیاست های خزش؛ • امنیت پایگاه داده ها؛ • ارزیابی فاکتورهای طراحی مثل پهنای باند، توان عملیاتی و پردازشی سرورها و غیره • حمله بهینه سازی جویس گر (SEO) وب گاه های آلوده؛ <p>آزمون نمایه ساز:</p> <ul style="list-style-type: none"> • فاکتورهای ساختمان داده؛ • آزمایش و ارزیابی فاکتورهای طراحی؛ • امنیت پایگاه داده ها؛ • آزمایش پارامتر زمانی دوره به روز رسانی نمایه ساز • آزمایش ماژول جستجو و موتور بازیابی در برابر انواع حملات تحت وب و داخلی؛ • حمله بهینه سازی جویس گر (SEO) و وب گاه های آلوده <p>آزمون رتبه بند:</p> <ul style="list-style-type: none"> • آزمایش و ارزیابی فاکتورهای طراحی • آزمایش و ارزیابی راهکارهای امنیتی مقابله با وب گاه های آلوده؛ <p>آزمایش راهکارهای امنیتی برای مقابله با حمله بهینه سازی جویس گر (SEO).</p>	<p>آزمون های زیر پس از توسعه نهایی مؤلفه های این بخش از مرحله توسعه، باید انجام شود. همچنین اگر پروژه وارد دور جدید چرخه حیات شود باید در برابر تهدیدهای جدید، بررسی و آزمایش شود (آزمایش جعبه سفید).</p> <ul style="list-style-type: none"> • آزمایش حملات منع خدمت (DoS)؛ • آزمایش حملات مرتبط با واسط کاربری جویس گر مانند بررسی نقاط ورودی؛ • بررسی امنیت پایگاه داده ها و مقاومت آن در برابر حملات شناخته شده؛ • آزمایش و ارزیابی فاکتورهای طراحی؛ • آزمایش پارامتر زمانی دوره به روز رسانی؛ • آزمایش ماژول های سرویس جویس گر در برابر انواع حملات تحت وب.
--	---	---	---	---

¹ Denial of Service

مرحله ۳- پیاده‌سازی / ارزیابی		خزش‌گر- نمایه‌ساز-رتبه‌بند	سرویس‌های تحت وب
Authorization	1. Create Detailed Plan for C&A تشکیل جزئیات صدور گواهی، مثل محدودیت پروژه، محدوده آزمایش، سطح دقت و غیره در آن مشخص می‌شود.	مسئلاً مجوز و گواهی انجام یک کار برای مرحله پیاده‌سازی در صورتی برای جویس‌گر و مؤلفه‌های آن ارائه می‌شود که تمام محدودیت‌ها و آزمایش‌های امنیتی لازم برای مؤلفه‌های اصلی جویس‌گر در مرحله توسعه به‌درستی انجام شده باشد. بنابراین اگر قرار باشد مجوز ادامه کار صادر شود، باید یک سند برنامه‌ریزی شده برای تمام محدودیت‌ها، وضعیت‌های آزمایشی و دقت مازول‌های خزش‌گر، نمایه‌ساز و رتبه‌بند ارائه شود؛ زیرا با وجود سند برنامه‌ریزی شده یکپارچگی اجزای جویس‌گر در مراحل بعدی به نحو بهتری انجام خواهد شد.	<ul style="list-style-type: none"> • حصول اطمینان از پیاده‌سازی و اجرایی کردن صحیح ملزومات، کنترل‌ها و روال امنیتی به‌منظور به‌کمینه‌رساندن تهدیدها و استفاده از گواهی معتبر منقضی‌نشده
	2. Integrate Security into Established Environments or Systems یکپارچه‌سازی سیستم‌های عملیاتی، تأیید کردن لیست کنترل‌های امنیتی اجرایی جهت فعال‌سازی	پس از اینکه مرحله توسعه برای سه مؤلفه اصلی تمام شد، فهرست سیاست‌های کنترلی و نظارتی امنیتی، تجزیه و تحلیل می‌شود و در نهایت این سیاست‌ها در مرحله بعد آزمایش و ارزیابی می‌شوند (فهرست کنترل‌های امنیتی شامل سیاست‌های خزش، سیاست‌های نمایه‌سازی، سیاست‌های رتبه‌بندی، سیاست‌های مربوط به مجوزدهی و کنترل‌های دسترسی در پایگاه داده‌ها و غیره می‌تواند باشد)؛	<ul style="list-style-type: none"> • تجزیه و تحلیل فهرست سیاست‌های کنترلی و نظارتی امنیتی و انجام آزمایش و ارزیابی سیاست‌های بالا در مرحله بعد • یکپارچه‌سازی و متمرکز کردن ویژگی امنیتی کنترل دسترسی به سرویس‌ها بر اساس سطوح دسترسی متناسب با اهمیت سرویس‌های طراحی شده
	3. Assess System Security ارزیابی امنیتی قبل از اعطاء مجوز، آزمایش‌های دوره‌ای و تأیید اثر بخشی کنترل امنیتی اجرایی، به‌روزرسانی طرح‌های امنیتی	<ul style="list-style-type: none"> • آزمایش بدهای امنیتی برای تک‌تک مازول‌ها (آزمایش جعبه سیاه) • تعیین آسیب‌پذیری‌ها و خطاهای نرم‌افزاری و سخت‌افزاری مربوط به مرحله توسعه برای بازگشت به ابتدای چرخه 	<ul style="list-style-type: none"> • آزمایش بدهای امنیتی برای تک‌تک مازول‌ها (آزمایش جعبه سیاه)؛ • تعیین آسیب‌پذیری‌ها و خطاهای نرم‌افزاری و سخت‌افزاری مربوط به مرحله توسعه برای بازگشت به ابتدای چرخه (استفاده از سکو، کامپایلر و تمامی ابزارهای توصیه‌شده و ابزارهای امنیت در توسعه چرخه حیات)؛ • تحلیل تمام توابع پروژه و APIها به‌منظور کاهش نقص‌های نرم‌افزاری امنیتی؛ • استفاده از فایل‌های سرآمد، کامپایلرهای جدید و ابزارهای پویا ایستا و پویای کدها به‌منظور بررسی کدهای موجود در توابع فهرست‌های ممنوعه و جایگزینی آن‌ها با موارد امن‌تر؛ • تحلیل اجرای ایستا، تحلیل منابع و کدهای اولیه برای کامپایل کردن، روش مقیاس‌پذیر مروری برکد امنیتی به‌منظور اطمینان حاصل کردن از کدگذاری امن.

¹ Application Programming Interface

	4. Authorize the Information System	اعطاء مجوزدهی سیستم اطلاعاتی برای پردازش، ذخیره، انتقال اطلاعات	<p>مسلماً بعد از پیاده‌سازی سامانه و قبل از عملیاتی شدن آن تمام فرایندهای مربوط به جمع‌آوری تا ذخیره‌سازی داده‌ها باید مشخص شوند و برای هر کدام از آن قسمت‌ها آزمایش‌های امنیتی انجام تا میزان درستی و اعتماد آن مازول‌ها ارزیابی شود و مجوز نهایی در صورتی به سامانه مربوطه ارائه می‌شود که بتواند در برابر انواع آزمایش‌ها ایمن باشد. برخی از جنبه‌های امنیتی که باید در این مرحله بررسی شود شامل محرمانگی، حریم خصوصی، صحت داده‌ها، کنترل دسترسی، امنیت ارتباط و دسترسی پذیری است.</p>	<ul style="list-style-type: none"> تهیه مدلی جهت کنترل دسترسی افراد به سرویس‌های طراحی و توسعه‌یافته جویس گره‌های بومی و ثبت رویدادها
مرحله ۴ - نگهداری / اجرا			سرویس‌های تحت وب	
Authentication, Robustness	1. Review Operational Readiness	<p>- بررسی آمادگی عملیاتی سامانه - همراه با زمان‌بندی و اعتباربخشی به فعالیت‌ها، - بررسی آمادگی اجرایی با توجه به هرگونه تغییر</p>	<ul style="list-style-type: none"> پیاده‌سازی سیاست‌های کلی برای پایداری و در دسترس بودن سامانه (برای سه مؤلفه اصلی) تعیین رویه‌ها و چارچوب‌های کاری برای تغییرات نرم‌افزاری و سخت‌افزاری در هر دوره از چرخه حیات تعیین مقیاس پذیر بودن سامانه و ارائه راه‌کارهای مربوطه برای افزایش مقیاس پذیری؛ پیاده‌سازی سامانه‌های نظارتی و کنترلی دائمی، برای جلوگیری از خرابی و ازدسترس خارج شدن سامانه 	<ul style="list-style-type: none"> پیاده‌سازی سیاست‌های کلی برای پایداری و در دسترس بودن سامانه؛ تعیین رویه‌ها و چارچوب‌های کاری برای تغییرات نرم‌افزاری و سخت‌افزاری در هر دوره از چرخه حیات؛ بررسی آمادگی اجرایی برای توسعه سرویس‌های جویس گره‌های بومی؛ تحلیل پویا و تأیید بلادرنگ سرویس با استفاده از ابزارهای پیش‌گر رفتارهای مخرب حافظه، موارد حق دسترسی کاربر و دیگر موضوعات امنیتی؛ مروری بر رویه حمله براساس تکمیل کد به‌منظور اطمینان حاصل کردن از تغییر در طراحی و پیاده‌سازی سامانه و یا سرویس مورد نظر؛ ایجاد بردار حمله با استفاده از موارد بالا؛ پیاده‌سازی سامانه‌های نظارتی و کنترلی دائمی، برای جلوگیری از خرابی و ازدسترس خارج شدن سرویس.
	2. Perform Configuration Management	<p>ضبط تغییرات و ارزیابی تأثیرات بالقوه آن بر سامانه (چون هر تغییر سخت‌افزاری و نرم‌افزاری می‌تواند بر امنیت مؤثر باشد)</p>	<p>مسائل مربوط به این بخش شامل سه مؤلفه اصلی می‌شود؛ زیرا به‌مرور زمان با افزایش تعداد درخواست‌ها و کاربران یا به‌وجود آمدن تهدیدهای جدید نیاز است که در سخت‌افزار و نرم‌افزار مؤلفه‌های اصلی جویس گر تغییراتی اعمال شود.</p> <p>تغییرات سخت‌افزاری بیشتر به مسئله مقیاس‌پذیری سامانه برمی‌گردد و تغییرات نرم‌افزاری به مسائل موزی‌سازی فرایندها برای بهبود سرعت جستجوها و راه‌کارهای امنیتی مربوط به رتبه‌بندی برای مقابله با حمله بهینه‌سازی جویس گر (SEO) اشاره می‌کند. در واقع راهکارهای امنیتی رتبه‌بند باید به‌طور دائمی در حال بهبود باشند.</p>	<p>با افزایش تعداد درخواست‌ها و کاربران یا به‌وجود آمدن تهدیدهای جدید نیاز است که در سخت‌افزار و نرم‌افزار مؤلفه‌های اصلی سرویس تغییراتی اعمال شود.</p>

	3. Conduct Continuous Monitoring	نظارت مداوم از اثربخشی کنترل امنیت در خود ارزیابی، مدیریت پیکربندی، مدیریت آنتی ویروس، مدیریت وصله، آزمایش امنیت، ارزیابی و یا ممیزی	<p>یک سامانه به دلیل وجود تهدیدهای جدید در طول زمان با تغییراتی همراه خواهد بود. بنابراین برای مقابله با تهدیدها و بهبود عملکرد امنیتی سامانه نیاز است که به طور پیوسته از گام‌های زیر استفاده کرد:</p> <ul style="list-style-type: none"> • بهره‌گیری از ابزارهای نظارتی و کنترلی در سه سطح خزش‌گر، نمایه‌ساز و رتبه‌بند برای جلوگیری از اثرات مخرب به سطوح دیگر؛ • استفاده از وصله‌های امنیتی برای پلتفرم سرورهای خزش‌گر، نمایه‌ساز و رتبه‌بند به طور دائمی؛ • بهره‌گیری از ضدبدافزارها و نرم‌افزارهای پالایش محتوا برای شناسایی وب‌گاه‌های آلوده در سطح مراحل خزش‌گر، نمایه‌ساز و رتبه‌بندی. 	<p>یک سامانه به دلیل وجود تهدیدهای جدید در طول زمان با تغییراتی همراه خواهد بود؛ بنابراین برای مقابله با تهدیدها و بهبود عملکرد امنیتی سرویس‌ها نیاز است که به طور پیوسته از گام‌های زیر استفاده کرد:</p> <ul style="list-style-type: none"> • بهره‌گیری از ابزارهای نظارتی و کنترلی برای جلوگیری از اثرات مخرب به سطوح دیگر؛ • استفاده و اعمال وصله‌های امنیتی در برنامه‌های اجراکننده سرویس‌ها؛ • بهره‌گیری از ضد بدافزارها و نرم‌افزارهای پالایش محتوا برای شناسایی وب‌گاه‌های آلوده؛ • آزمایش فازی که عبارت از استنتاج خرابی برنامه با معرفی داده‌های تصادفی و نامتعارف است.
مرحله ۵- امحاء		خزش‌گر - نمایه‌ساز - رتبه‌بند	سرویس‌های تحت وب	
Access Control-Authorization	1. Build and Execute Disposal or Transition Plan	طرح خاتمه یا انتقال سامانه	<p>پس از توسعه و پیاده‌سازی تمام ماژول‌های جویس‌گر نوبت به گزارش‌دهی و ارائه اطلاعات تکمیلی از روند کار است. بنابراین طرح جامع اطلاعاتی که نشان‌دهنده تمام شدن مراحل پروژه است، باید در این بخش از مرحله، به صورت مکتوب ارائه شود.</p> <p>همچنین در این بخش از مرحله، برای کاهش هزینه‌ها و ریسک‌های احتمالی قابلیت انتقال پروژه برای انجام آن بررسی می‌شود. در این بخش اگر قرار است که تمام یا بخشی از مراحل پروژه منتقل شود، باید دلایل و مستندات کافی ارائه شود تا در نهایت عملیات انتقال سامانه یا بخشی از آن صورت گیرد.</p>	<ul style="list-style-type: none"> • تشخیص مخاطبان اضطراری امنیت و تهیه طرح سرویس امنیت برای کدهای موروثی از دیگر گروه‌های سازمانی و کد شخص ثالث؛ • مستندسازی تمام و یا بخشی از اطلاعات پروژه با دلایل و مستندات کافی؛ • شناسایی، محاسبه ریسک‌های احتمالی و مدیریت ریسک‌ها؛ • حفظ و ذخیره اطلاعات حیاتی مانند طرح‌های امنیتی و نیازمندی‌های کنترل امنیت به طور منظم؛ • ساخت و اجرای طرح واگذاری/ انتقال محصول جویس‌گرهای بومی.
2. Ensure Information Preservation	الزامات قانونی، نمایه‌سازی اطلاعات و محل نگهداری آن‌ها و خصوصیشان (پایگاه داده‌ها)	<p>پایگاه داده‌ها علاوه بر امن بودن وضعیت دسترسی‌های فیزیکی و منطقی، باید زیرساخت امن نیز داشته باشند. برخی از الزاماتی که باعث امن شدن ذخیره‌سازی داده‌های هر مرحله می‌شود به شرح زیر است:</p> <ul style="list-style-type: none"> • ایمنی داده‌های موجود در پایگاه داده نسبت به مخاطرات فیزیکی؛ • قرارگیری پایگاه داده‌ها در زیرساخت‌های قابل اطمینان مثل IDC؛ • اعمال سیاست‌های امنیتی در هنگام ذخیره‌سازی (این سیاست‌ها در مرحله نخست مشخص شده‌اند)؛ • تهیه طرح پاسخ به رویدادها به منظور نشان‌دهی تهدیدهای جدید در طول زمان 	<p>برخی از الزاماتی که باعث امن شدن ذخیره‌سازی داده‌های هر مرحله می‌شود به شرح زیر است:</p> <ul style="list-style-type: none"> • ایمنی داده‌های موجود در پایگاه داده سرویس‌ها نسبت به مخاطرات فیزیکی؛ • قرارگیری پایگاه داده سرویس‌های مهم در زیرساخت‌های امن؛ • اعمال سیاست‌های امنیتی در هنگام ذخیره‌سازی (این سیاست‌ها در مرحله نخست مشخص شده‌اند)؛ • بایگانی اطلاعاتی نظیر: مشخصات، کدهای مرجع، باینری‌ها، نشانه‌های خصوصی، مدل-های تهدید، مستندسازی، طرح‌های پاسخ اضطراری، گواهینامه و خدمات شخص ثالث 	

3. Sanitize Media	جلوگیری از دسترسی‌های غیرمجاز به اطلاعات بایگانی شده	<p>پس از اینکه اطلاعات حاصل از هر مرحله به صورت فیزیکی یا دیجیتال مستند شد و در محل‌های ذخیره‌سازی و پایگاه داده‌های مربوطه قرار گرفت، باید یکسری سیاست امنیتی اعمال کرد که هر کاربر یا مازولی به اطلاعات نمایه‌شده دسترسی پیدا نکند. سیاست‌های کلی بدین صورت است:</p> <ul style="list-style-type: none"> • تصدیق اصالت و هویت‌شناسی کاربران داخلی و خارجی؛ • محدود کردن دسترسی‌های فیزیکی به منابع پایگاه داده‌ای و محل‌های ذخیره‌سازی؛ • ارائه یک شمای کلی از اطلاعات نمایه‌شده و دادن سطوح دسترسی عمومی به کاربران به طوری که امنیت اطلاعات به مخاطره نیفتد. 	<p>مستندسازی اطلاعات حاصل از هر مرحله به صورت فیزیکی یا دیجیتالی و قرارگرفتن آن‌ها در محل‌های ذخیره‌سازی و پایگاه داده‌های مربوطه، باید با اعمال سیاست‌های امنیتی مانع دسترسی هر کاربر یا مازولی به اطلاعات مهم شود. سیاست‌های کلی بدین صورت است:</p> <ul style="list-style-type: none"> • تصدیق اصالت و هویت‌شناسی کاربران داخلی و خارجی در استفاده از انواع سرویس‌های جویش‌گرهای بومی؛ • محدود کردن دسترسی‌های فیزیکی به منابع پایگاه داده‌ای و محل‌های ذخیره‌سازی اطلاعات مهم سرویس‌ها • ارائه یک شمای کلی از اطلاعات و دادن سطوح دسترسی عمومی به کاربران مصرف‌کننده سرویس‌های جویش‌گرهای بومی به طوری که امنیت اطلاعات به مخاطره نیفتد
4. Dispose of Hardware and Software	بررسی وضعیت فروش، اهدا یا امحا سخت‌افزار و نرم‌افزار سامانه قبل	<ul style="list-style-type: none"> • پیاده‌سازی سیاست‌های مربوط به امحای اطلاعات در سامانه توسعه‌یافته • اعمال سیاست‌های انتقال نرم‌افزار و سخت‌افزار در سامانه پیاده‌سازی شده 	<ul style="list-style-type: none"> • پیاده‌سازی سیاست‌های مربوط به امحای اطلاعات سرویس‌های قبلی
5. Close System	خاتمه سامانه با مجوز نهایی	<ul style="list-style-type: none"> • بایگانی و طبقه‌بندی کردن تمام اطلاعات سامانه • ارائه مجوز شروع به کار سامانه توسعه‌یافته • پاسخ‌گویی مناسب به گزارش‌های آسیب‌پذیری‌ها و تهدیدهای سرویس • توانایی پیاده‌سازی طرح پاسخ‌گویی رویداد به منظور حفاظت از مشتریان در برابر آسیب‌پذیری‌های حریم خصوصی و امنیت سرویس 	<ul style="list-style-type: none"> • بایگانی و طبقه‌بندی کردن تمام اطلاعات سامانه • ارائه مجوز شروع به کار سامانه توسعه‌یافته • پاسخ‌گویی مناسب به گزارش‌های آسیب‌پذیری‌ها و تهدیدهای سرویس • توانایی پیاده‌سازی طرح پاسخ‌گویی رویداد به منظور حفاظت از مشتریان در برابر آسیب‌پذیری‌های حریم خصوصی و امنیت سرویس

۵- نتیجه‌گیری

لحظه امحا بر روی آن اعمال شود. این مقاله بر مبنای بررسی و مطالعات منابع موجود و استانداردهای مرتبط، توانسته است، شاخص‌های ارزیابی امنیتی را متناسب با مؤلفه‌های اصلی امنیتی در هر یک از مرحله‌های چرخه حیات یک نمونه از سامانه‌های اطلاعاتی مانند جویش‌گر بومی در قالب یک چارچوب جامع عملیاتی ارائه کند؛ زیرا جهت برقراری و تداوم امنیت در این گونه سامانه‌ها لازم است با استفاده از چارچوب پیشنهادی (که در قالب جدول

همانطور که اشاره شد برای ایمن‌سازی سامانه‌های اطلاعاتی و سرویس‌های تحت وب می‌بایست، ابتدا به شناسایی اصول و ابزارهای کنترل امنیتی و چارچوب‌ها و الگوهای امنیتی آن پرداخت، این ابزارهای کنترلی، عملیاتی، فنی و یا مدیریتی می‌توانند باشند. مرحله بعدی، استخراج اصول اولیه ایمن‌سازی سرویس، مشتمل بر شناسایی، تشخیص و مدل‌سازی تهدیدها درخصوص هر سامانه است که باید بر مبنای چرخه حیات توسعه سامانه از لحظه پیدایش تا

- [11] Roudies, Ounsa. "Benchmarking SDL and CLASP lifecycle." Intelligent Systems: Theories and Applications (SITA-14), 2014 9th International Conference on. IEEE.
- [12] Chess, Brian, and Brad Arkin. "Software security in practice." Security & Privacy, IEEE 9.2 (2011): pages89-92.
- [13] Yasar, Ansar-Ul-Haque, et al. "Best practices for software security: An overview." Multitopic Conference, 2008, INMIC 2008. IEEE International. IEEE.
- [14] Solinas, Marco, Leandro Antonelli, and Eduardo Fernandez. "Software secure building aspects in Computer Engineering." Latin America Transactions, IEEE (Revista IEEE America Latina) 11.1 (2013), pages 353-58
- [15] Talukder, Asoke K., et al. "Security-aware software development life cycle (sasdlc)-processes and tools." Wireless and Optical Communications Networks, 2009. WOCN'09. IFIP International Conference on. IEEE, 2009.
- [16] Noopur Davis. "Secure Software Development Life Cycle Processes". Retrieved from: <https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/sdlc/326-BSI.html>. 2017.
- [17] Thomassen, Pal. "Software Security State of the theory vs state of the practice." Software Engineering Institute. 2006-07-05; Updated (2012).
- [18] Microsoft patterns & practices –security fundam-entals for web services- chapter 1
- [19] Nasrin Taj, Shaghayegh Naderi "Evaluation of Security Indicators in the Life Cycle of Information Systems Development", 1st International Conference on New Advances in Electrical and Computer Engineering, Amir Kabir University of Technology, 2016/4/14.

سه‌بعدی (۱) ارائه شده) بازخوردهای عملیاتی مؤلفه‌های اصلی امنیت و شاخص‌های ارزیابی و نحوه تأثیرگذاری آن‌ها بر یکدیگر در هر مرحله از چرخه حیات را استخراج کرده و مورد ارزیابی قرار داد [19].

۶- مراجع

- [1] Geer, David. "Are companies actually using secure development life cycles?" Computer (Volume: 43, Issues:6,7 June 2010 ,pages 12-16)
- [2] Nelson, Paul, (Chief Architect at Search Technologies) "A Reference Architecture for Document-Level Security in Search Systems", <http://www.searchtechnologies.com/search-engine-security-architecture2017>.
- [3] Nelson, Paul, "Everything You Ever Wanted to Know about Search Engine Security", <http://www.searchtechnologies.com/search-engine-security.2017>
- [4] Security Consideration in the System Development Life Cycle- National Institute of Standard and Technology 800-64 Revision 2- October
- [5] Security and Privacy Controls for Federal Information Systems and Organizations- National Institute of Standard and Technology 800-53 Revision 4- April 2013
- [6] Management Information Security Risk- National Institute of Standard and Technology 800-39 March 2011
- [7] Khan, Muhammad Umair Ahmed, and Mohammed Zulkernine. "On selecting appropriate development processes and requirements engineering methods for secure software." Computer Software and Applications Conference, 2009. COMPSAC'09. 33rd Annual IEEE International. Vol. 2. IEEE, 2009. pages 353-358.
- [8] Pakdeetrakulwong, Udsanee, Pornpit Wongthongtham, and Waralak V. Siricharoen. "Recommendation systems for software engineering: A survey from software development life cycle phase perspective." Internet Technology and Secured Transactions (ICITST), 8-10 dec, 2014 9th International Conference for. IEEE,
- [9] Apvrille, Axelle, and Makan Pourzandi. "Secure software development by example." IEEE Security & Privacy 4 (2005): pages10-17.
- [10] Lipner, Steve. "Security development lifecycle." Datenschutz und Datensicherheit- DuD 34.3 (2010): pages135-137.

[19] نسرين تاج، شقایق نادری "ارزیابی شاخص‌های امنیتی در چرخه حیات توسعه سیستم‌های اطلاعاتی" اولین کنفرانس بین المللی دستاوردهای نوین پژوهشی در مهندسی برق و کامپیوتر، دانشگاه صنعتی امیرکبیر، ۹۵/۲/۲۳



نسرين تاج فارغ التحصيل کارشناسی ارشد مهندسی فناوری اطلاعات 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 اطلاعات، امنیت جویسگر بومی و مدیریت فناوری اطلاعات است و تاکنون بیش از ده‌ها مقاله در مجلات علمی پژوهشی و کنفرانس‌های داخلی و خارجی به چاپ رسانیده است.



شقایق نادری کارشناسی خود را در مهندسی کامپیوتر از دانشگاه خوارزمی دریافت کرد. تحصیلات کارشناسی ارشد و دکترای خود را در رشته مهندسی کامپیوتر گرایش نرم‌افزار از دانشگاه

تربیت مدرس به ترتیب در سال‌های ۱۳۸۱ و ۱۳۹۱ به پایان رسانده است. وی در حال حاضر استادیار پژوهشگاه ارتباطات و فناوری اطلاعات است. زمینه‌های پژوهشی مورد علاقه ایشان یادگیری ماشین و امنیت سامانه‌های چندرسانه‌ای است.



مهسا امیدوار سرکندی مدرک کارشناسی خود را در رشته مهندسی کامپیوتر گرایش نرم افزار در سال ۱۳۹۳ از دانشگاه آزاد اسلامی واحد تهران جنوب دریافت کرد. وی هم‌اکنون

دانشجوی رشته کارشناسی ارشد نرم‌افزار دانشگاه صنعتی امیرکبیر است. زمینه‌های پژوهشی مورد علاقه ایشان امنیت نرم‌افزار، ارزیابی آسیب‌پذیری و تهدیدهای برنامه‌های کاربردی، تحلیل و طراحی نرم افزارهای امن و پایگاه‌های تحت ابر است.



حسن کوشکی 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 رایانه‌ای، امنیت چندرسانه‌ای، جریان‌سازی مدیا روی اینترنت، جریان‌سازی ویدیو نظیر به نظیر، امنیت سامانه‌های مبتنی بر شهرت و طراحی امن معماری شبکه است.