

ارائه شاخص‌های امنیتی در چرخه حیات توسعه

سامانه جوش‌گرد بومی

نسرين تاج نيشابوري^{۱*}، شقايق نادری^۲، مهسا اميدوار سركندي^۳ و حسن کوشکي^۴

^۱کارشناس 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 و ^۴ 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 دسترسی‌پذیری بالا، در جوش‌گرهای بومی قابل تأمل و بررسی است؛ از این‌رو معرفی و نحوه به کارگیری ابزارهای کنترل امنیتی در مؤلفه‌ها و اجزای اصلی جوش‌گرهای بومی مانند خوش‌گر، رتبه‌بند و نمایه‌ساز، به همراه ملاحظات امنیتی سرویس‌های تحت وب جوش‌گر در تمامی مراحل چرخه حیات توسعه جوش‌گرهای بومی، اصلی‌ترین محور این مقاله را تشکیل می‌دهد. این مقاله سعی دارد با بررسی استانداردهای امنیتی مرتبط با چرخه حیات توسعه یک سامانه و با درنظرگرفتن اجزای تشکیل‌دهنده کلیدی جوش‌گرهای بومی، نحوه ترکیب تمامی این ابعاد را در چرخه حیات توسعه جوش‌گرهای بومی معرفی کرده تا طراحان، با اعمال صحیح و به موقع ملاحظات و کنترل‌های امنیتی، بتوانند به بهره‌برداری این‌من و با کیفیتی از مؤلفه‌ها و اجزای اصلی جوش‌گرهای بومی دست یابند.

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

۱- مقدمه

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 جوش‌گرهای بومی با رعایت و اعمال این موارد، بتوانند بهره برداری امن و باکیفیتی از مؤلفه‌ها و اجزای اصلی جوش‌گرهای بومی ارائه کنند [2]. [3].

۲- نحوه اعمال ابزارهای کنترلی در امن‌سازی سرویس‌های جوش‌گرهای بومی

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 مشاهده شده [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 جوش‌گرهای بومی مانند خوش‌گر، رتبه‌بند، نمایه‌ساز و ملاحظات امنیتی در سرویس‌های تحت وب در جوش‌گرهای بومی در تمامی مراحل چرخه حیات توسعه جوش‌گرهای بومی است. این مقاله با بررسی

* نویسنده عهده‌دار مکاتبات

قابلیت‌های پیچیده‌تر با یکدیگر می‌توانند ترکیب شوند و محل ارائه آن‌ها بر روی اینترنت، اینترانت 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 به‌اجمال، 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 جویش‌گرهای بومی مبتنی بر وب هستند. لحاظ کردن امنیت در طول چرخه حیات توسعه سامانه از ابزار اصلی ایجاد امنیت در جویش‌گرهای بومی است؛ زیرا در طی این عمل با استفاده از مدل تهدیدها طراحی بخش‌های مختلف مانند کد، استقرار و آزمایش را می‌توان بهبود بخشد [5].

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

بر طبق بررسی‌های به عمل آمده، 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 هدايت و برنامه‌ریزی ناصحیح دوران بی‌حاصیل آن پدیدار شده و درنهایت 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 گروه 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 روش است که به کارگیری آن موجب کاهش مخاطرات در یک سامانه می‌شود. به عبارت دیگر برای کاهش مخاطرات حاصل از هر تهدید، لازم است از یک با چند ابزار کنترلی استفاده شود؛ همچنین ممکن است یک کنترل ساده یا مرکب به‌منظور کاهش مخاطره ناشی از چند تهدید هم‌زمان، به کارگرفته 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]. قبل از بررسی سرویس‌های امنیتی مورد نیاز در جویش‌گرهای بومی لازم است به‌اجمال به مفهوم امن‌سازی در سرویس‌ها بپردازیم. امنیت به‌طور اساسی 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 به‌طور کامل 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. در حقیقت امنیت همان مدیریت ریسک و اجرای اقدامات متقابل و مؤثر است و امنیت مؤثر ترکیبی از مردم، فرآیند، و فناوری است. امنیت متنکی بر ارکان: احراز هویت، مجاز شماری، حساب‌رسی و انکار ناپذیری، محروم‌بودن، تمامیت و یکپارچگی و در دسترس بودن 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 جویش‌گرهای بومی، یک سامانه اطلاعاتی تحت وب هستند که هدف اصلی آن هدایت کاربران در دستیابی بهتر به اطلاعات مورد نیاز است؛ لذا با لحاظ‌کردن این دستورالعمل در جویش‌گرهای 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 دسترس پذیری، همچنین الحال 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، پیکربندی نامناسب و پیاده‌سازی کنترل امنیت با قیمت کمتر و کاهش آسیب‌پذیری‌ها؛
- افزایش کنترل امنیتی با آگاهی از چالش‌های مهندسی؛
- مشخص کردن سرویس‌های امنیتی به‌اشتراک گذاشته شده 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 درجهت ترویج سرمایه‌گذاری؛
- جلوگیری از اختلالات بعدی با افزایش ایمنی در تعاملات بین سامانه‌ای.

همان‌طور که گفته شد، استاندارد NIST SP 800-64 با رویکرد ریسک محور 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 تمهداتی که باید در آینده صورت گیرد، می‌توان به دست 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 پیش‌بینی شده 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؛ به عبارتی امن‌کردن 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 به صورت ترکیبی استفاده می‌شوند؛ به عنوان مثال امنیت چرخه حیات توسعه سامانه با امنیت چرخه حیات توسعه نرم‌افزار که با توجه به اجزای تشکیل‌دهنده جویش‌گرهای بومی، می‌توان گفت امنیت چرخه حیات توسعه سامانه و امنیت چرخه حیات توسعه نرم‌افزار در حفظ و ابقاء سامانه‌های جویش‌گرهای بومی با توجه به ماهیت تکوین و خروجی‌های مورد انتظار آن بهشت 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 به طور همزمان در طی چرخه توسعه حیات جویش‌گرهای 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. درنتیجه 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 جویش‌گرهای بومی ارائه کرد تا جایگاه آن‌ها در هنگام بررسی این استاندارد، مشخص شود. جویش‌گرهای بومی ترکیبی از سخت‌افزارها و نرم‌افزارهایی است که تحت

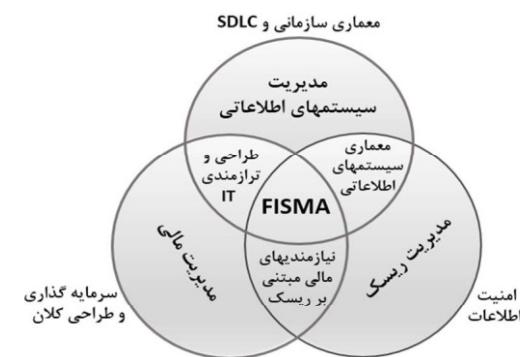
^۱ SDLC(Secure Development Life Cycle)

دو فصل نامه علمی ترویجی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)

• انجام^۳ BIA یا تجزیه تحلیل تأثیر کسب و کار و ارتباط آن با کارایی سامانه جهت مشخص سازی ارتباط سامانه و دارایی‌ها با سرویس‌های حساس و بررسی پیامدهای ناشی از اختلال آن‌ها؛ مدیریت ریسک و مدیریت منابع مالی نیز در بخش نیازمندی‌های مالی مبتنی بر ریسک با یکدیگر مشترکند. در دیدگاه مدیریت ریسک در استاندارد NIST SP 800-39 در رویکرد سامانه‌ای / سازمانی به تشریح یک چارچوب از مدیریت ریسک‌های امنیتی در سامانه‌های اطلاعاتی پرداخته شده است. همچنین این استاندارد به دنبال برقراری تعادل در حفاظت از دارایی‌ها و اطلاعات سامانه / سازمان با راهبرد کنترل هزینه و کاهش ریسک در طی چرخه حیات توسعه سامانه است. درخصوص این استاندارد در بخش‌های بعدی توضیح داده خواهد شد. در بخش تداخل حوزه مدیریت فناوری اطلاعات و مدیریت منابع مالی باید دانست که مؤثرترین راه برای پیاده‌سازی مدیریت ریسک، مشخص کردن عملیات و دارایی‌های حساس و آسیب‌پذیری‌های نظاممند است. ریسک‌ها مشترک هستند و توسط سازمان، منابع درآمد یا تپیلوژی سازمان محدود نمی‌شوند. مشخص کردن عملیات و اصلاح منابع حساس و ارتباطات بین این دو از طریق فرآیند طراحی امنیت سامانه و تدوین اطلاعات حاصل می‌شود. دو فرایند CPIC به معنی برنامه‌ریزی و کنترل سرمایه‌گذاری و EA به معنای معماری سازمانی در ایجاد این دیدگاه در عملیات مهم تجاری یک سازمان دخیلنده. آن‌ها از دارایی‌های یک سامانه یا سازمان پشتیبانی کرده و وابستگی‌ها و ارتباطات را به وجود می‌آورند. با مشخص کردن عملیات و دارایی‌های حساس، سازمان‌ها می‌توانند یک BIA یا تجزیه تحلیل تأثیر کسب و کار انجام دهنند. هدف از BIA ارتباط سامانه و دارایی‌ها با سرویس‌های حساس و بررسی پیامدهای ناشی از اختلال آن‌ها است. برای اساس در یک سامانه / سازمان تأثیرات امنیت را بر روی اولویت‌ها می‌توان مدیریت کرد. این کار برای آسان‌کردن برنامه‌هایی درخصوص کارایی هزینه، تأثیرات تجارت و ارزش آن برای سازمان یا سامانه است. با دیدگاه مدیریت ریسک در یک سامانه یا یک پروژه، امنیت CPIC^۲ از همان ابتدا در سرتاسر سامانه و چرخه حیات وجود دارد. با این کار نقش برجسته‌ای از اندازه‌گیری و تحمیل نیازمندی‌های امنیتی در سرتاسر مرحله‌های چرخه حیات مستند خواهد شد. مدیران از این اطلاعات در

در جهت مدیریت و توسعه فناوری اطلاعات از آن استفاده می‌شود. برای اساس حوزه‌های مدیریت سامانه‌های اطلاعاتی، مدیریت ریسک و مدیریت منابع مالی در انجام این فعالیت به صورت سه‌گانه با یکدیگر درگیر می‌شوند که این تداخل در شکل (۱) نشان داده شده است:

در بخش مدیریت سامانه‌های اطلاعاتی، معماری و چرخه حیات توسعه سامانه (SDLC) شکل می‌گیرد و در تداخل با حوزه مدیریت ریسک، وارد بخش معماری سامانه‌های اطلاعاتی و چارچوب FISMA می‌شود. همچنین در تداخل با حوزه مدیریت مالی، وارد بخش طراحی و ترازندهای پژوهش‌های فناوری اطلاعات شده و دوباره از چارچوب FISMA استفاده می‌شود.



(شکل-۱) ترکیب حوزه‌های مدیریتی با سیستم‌های اطلاعاتی [۴]

• 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 (EA)^۱.
- مشخص کردن معماری سامانه‌ای؛ با استفاده از مدیریت ریسک و چارچوب FISMA.
- بودجه‌بندی و طراحی بخش‌های مختلف یک سامانه براساس مدیریت منابع مالی و انجام CPIC^۲.
- مشخص کردن عملیات و دارایی‌های حساس و آسیب‌پذیری‌های سامانه جهت الویت‌بندی‌های مالی و بالابردن آمادگی ریسک‌پذیری آن؛

¹ Enterprise Architecture

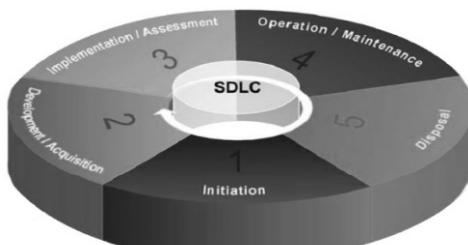
² Capital Planning and Investment Control

³ Business Impact Analysis

استاندارد NIST SP 800-53,39 محروم‌گی، یکپارچگی و دسترس‌پذیری سامانه‌های اطلاعاتی امکان‌پذیر خواهد بود. با استناد به این استاندارد، جویش‌گرهای 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 جویش‌گرهای بومی را پشتیبانی و تقدیم می‌کند. آشکار شود. به‌طور معمول این معماری با انجام زمان‌بندی مناسبی از وظایف، فعالیت‌های مورد انتظار، تخمین منابع مورد نیاز جویش‌گرهای 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 تجمعیغ 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

خودیادآوری و چرایی تصمیمات گرفته شده و ارزیابی بیشتر آن می‌توانند استفاده کنند. همچنین گروه‌های حسابرسی و نظارت نیز از این اطلاعات در بازنگری برای اصلاح مدیریت سیستم و مشخص کردن نقاطی که امنیت در آن نقاط نادیده گرفته شده می‌توانند استفاده کنند؛ همچنین می‌توانند 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 توسعه یافته و ساخته می‌شود.

- ارزیابی/ پیاده‌سازی: پس از آزمایش موفقیت‌آمیز سامانه، نصب آن انجام می‌شود؛
 - تغییراتی/ اجرا: در طی این مرحله سامانه کار تعیین شده را انجام داده، مورد بهره‌برداری قرار می‌گیرد و توسط افروند سخت‌افزار و نرم‌افزار و حوادث دیگر اصلاح می‌شود؛
 - امتحان: فعالیت‌های انجام شده در طی این مرحله اطمینان می‌دهد که سامانه به‌طور منظم خاتمه یافته و امتحان می‌شود، حفظ اطلاعات حیاتی سامانه و انتقال داده‌های پردازش شده توسط سامانه به سامانه جدید و حفظ آن مطابق سیاست‌ها و قوانین مدیریتی قبل اجرا از وظایف این مرحله است. در هریک 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 تحويل 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 جویش‌گرهای بومی منجر به تشکیل بهتر EA و CPIC می‌شود، که همان‌طور که در قسمت‌های قبل گفته شد، به‌منظور مشخص شدن معماری داخلی جویش‌گرهای بومی و تأمین منابع مالی آن مورد نیاز خواهد بود.

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

فعالیت‌های امنیتی افزوده شده به مرحله توسعه/ اکتساب شامل:

- ارزیابی ریسک‌ها و استفاده از این نتایج به عنوان مکملی برای کنترل امنیتی پایه در جویش‌گرهای بومی؛
- تحلیل نیازمندی‌های امنیتی جهت برطرف کردن گپ‌ها یا افزونگی‌های بلااستفاده در جویش‌گرهای بومی؛
- انجام توابع و آزمایش‌های امنیتی جویش‌گرهای بومی به‌منظور امکان اعمال بازخورد و برگشت به مراحل قبل؛
- آماده کردن مستندات اولیه برای تأیید و گواهی بخشیدن به سامانه جویش‌گرهای بومی؛
- طراحی معماری امنیتی به صورت گرافیکی و با جزئیات به‌نحوی که مکان و چگونگی کنترل‌های امنیتی در آن نشان داده شود. خلاصه این معماری و راهبردهای لحاظ شده در طراحی امنیتی سامانه جویش‌گرهای 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 به طور ثابت بازخورد گرفته تا به تدریج کامل شود. مستندات امنیتی در جویش‌گرهای بومی باید با موارد زیر تراز شود:
- تحلیل نیازمندی‌های امنیتی [7] جویش‌گرهای بومی
- معماری امنیتی جویش‌گرهای بومی؛
- ارزیابی تأثیرات کسب و کار و طبقه‌بندی امنیتی اطلاعات در جویش‌گرهای بومی.

گرفته‌اند. امنیت در این نقطه مطابق ریسک‌های کسب و کار، اطلاعات اداره امنیت اطلاعات مشخص شده‌اند. به عنوان 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 جویش‌گرهای بومی از نظر محرومگی، صحت و دسترس پذیری تشریح شود که خروجی آن آموزش امنیتی تیم توسعه‌دهنده و طرح‌های تضمین کیفیت در سامانه و استانداردهای کدنویسی و توسعه سامانه جویش‌گرهای بومی خواهد بود. همچنین راهبردهای کسب و کار مشخص می‌شوند. باید اطمینان حاصل کرد که ذی‌نفعان درگیر در سامانه خدمات جویش‌گرهای 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 جویش‌گرهای بومی و مشخصه‌هایی که برای انتقال و ذخیره‌سازی اطلاعات به کار گرفته می‌شود، نظریه 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 جویش‌گرهای بومی.
- نتیجه یک طراحی آگاهانه و به موقع، صرفه‌جویی در وقت و هزینه و طراحی مناسب در مدیریت ریسک جویش‌گرهای بومی است. مباحث امنیتی به عنوان بخشی از توسعه سامانه باید به کار گرفته شوند (نه به صورت مجزا). کارکنان یک سازمان یا کاربران جویش‌گرهای بومی باید بدانند که برخورد متقاطعی 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

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

۳-۵ مرحله پنجم چرخه حیات توسعه

سامانه و ملاحظات امنیتی وابسته به آن

مرحله آخر توسعه جویش‌گرهای بومی در معرض استفاده قرارگرفتن محصول است. در مرحله پنجم این هنگام انتقال در سامانه‌های اطلاعاتی باید از حفاظت منابع دولتی و دارایی‌های آن اطمینان حاصل کرد. به طور معمول هیچ نقطه مشخصی به عنوان پایان یک سامانه وجود ندارد. هر سامانه‌ای به دلیل پیشرفت فناوری و تغییر نیازمندی‌ها ناگزیر است که به سمت نسل بعدی خود در حال حرکت باشد. لذا طراحی امنیت جویش‌گرهای بومی باید به طور 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 به طور منظم با حفظ و ذخیره اطلاعات حیاتی نظری 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 پردازش شده 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 محصل
- جویش‌گرهای بومی
- بایگانی اطلاعات حیاتی سامانه جویش‌گرهای بومی
- حفاظت از استناد و مدارک حیاتی در محیط یا رسانه و طبقه‌بندی آن که منجر به مشخص کردن سطح ریسک‌های سامانه جویش‌گرهای بومی می‌شود.

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^۱ C&A؛
- یک پارچگی‌سازی امنیت در داخل محیط یا سامانه مربوطه که خروجی آن اصلاح فهرست کنترل‌های امنیتی اجرایی جویش‌گرهای بومی است.
- تأمین امنیت سامانه دسترسی که خروجی آن گزارش ارزیابی امنیتی جویش‌گرهای بومی و بسته احراز اصالت امنیتی و ورودی برای^۲ POA&M^۳ است.
- الزام استفاده از سامانه اطلاعات احراز اصالت به‌منظور تصمیم‌گیری‌های امنیتی در جویش‌گرهای بومی؛
- هماهنگی کامل میان طراحی و انجام فعالیت‌های گواهی و تأیید سامانه با آزمایش کنترل امنیت جویش‌گرهای بومی که خروجی آن بازنگری مالی، بهروزرسانی آن، بررسی آمادگی توسعه سامانه جویش‌گرهای 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 افزوده شدن یا جایگزینی هستند. در این مرحله جویش‌گرهای بومی نیز باید براساس نیازهای امنیتی مورد بررسی قرار گیرد تا به عملکرد مفید خود ادامه دهد. سامانه عملیاتی شده به طور مرتب در حال بازبینی به‌منظور اطمینان حاصل کردن از عملکردشان با توجه به نحوه پاسخ‌دهی به نیازهای یک سازمان در مرحله نگهداری و به‌هنگام خطرهای توافق‌شده کاراتر و امن‌تر هستند. فقط در صورت اصلاح و تغییرات این مرحله، جویش‌گرهای بومی به مرحله می‌توانند بروند. بنابراین فعالیت‌های پیوستی امنیتی در این مرحله شامل: بررسی آمادگی اجرایی برای توسعه جویش‌گرهای بومی.

¹ Certification and accreditation

² Plan of Action and Milestone

دو فصل نامه علمی ترویجی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)

همچنین بر مبنای کنترل‌های امنیتی و خروجی‌های مورد انتظار در هر مرحله، شاخص‌های امنیتی اصلی در هر مرحله از چرخه حیات را در هریک از اجزا و ساختار معماری جویش‌گرهای بومی و سرویس‌های تحت وب به بحث گذاشتیم. درنهایت جدول سه‌بعدی که متشکل از اجزای اصلی جویش‌گرهای بومی، سرویس‌های تحت وب و مرتبط با آن، مؤلفه‌های امنیتی و شاخص‌های ارزیابی امنیتی در هریک 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 جویش‌گرهای بومی می‌تواند باشد. [16] نتیجه پژوهش‌ها و مطالعات بالا در قالب جدول (۱) آورده شده است.

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

۴- استخراج شاخص‌های امنیتی در چرخه حیات امن جویش‌گرهای بومی

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

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

مؤلفه‌های امنیتی مورد تأکید		فعالیت‌های امنیتی در چرخه حیات توسعه سامانه	
مرحله ۱- شروع		خوش‌گر- نمایه‌ساز- رتبه‌بند	سرویس‌های تحت وب
Robust,Trust,CIA	1. Initiate Security Planning زمانبندی فعالیت‌های امنیتی از نظر تقدیم و تأخیر	<p>در هنگام توسعه یک سامانه به دلیل مازولار کردن بخش‌ها باید فعالیت‌ها و سیاست‌های امنیتی در هر کدام از بخش‌ها به صورت مجزا اعمال شود به طوری که در هر بخش مسائل امنیتی با درجه اهمیت بالاتر باید زودتر پیاده‌سازی شوند. زمان‌بندی فعالیت‌های امنیتی به صورت سلسه‌مراتبی برای سه مؤلفه اصلی جویش‌گر به شرح زیر است:</p> <ul style="list-style-type: none"> خوش‌گر: <ul style="list-style-type: none"> توسعه الگوریتم‌های خوش‌گر و سیاست‌های امنیتی موجود در آن‌ها پیاده‌سازی فاکتورهای طراحی نرم‌افزاری و ساختافزاری خوش‌گر پیاده‌سازی پایگاه داده خوش‌گر نمایه‌ساز: توسعه الگوریتم‌های نمایه‌سازی و سیاست‌های امنیتی موجود در آن‌ها پیاده‌سازی فاکتورهای طراحی نرم‌افزاری و ساخت افزاری نمایه‌ساز پیاده‌سازی پایگاه داده نمایه‌ساز رتبه‌بند: <p>در توسعه یک سرویس به دلیل مازولار کردن بخش‌ها باید فعالیت‌ها و سیاست‌های امنیتی در هر کدام از بخش‌ها به صورت مجزا اعمال شود؛ به طوری که در هر بخش مسائل امنیتی با درجه اهمیت بالاتر باید در اولویت قرار گیرد. زمان‌بندی فعالیت‌های امنیتی سرویس به شرح زیر است:</p> <ul style="list-style-type: none"> مروری بر مفاهیم اصلی امنیت در چرخه حیات سرویس‌های تحت وب تئیه 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 ساخت افزاری انتخاب رویکردها و روش‌های امن در پایگاه داده شناسایی و ارزیابی ریسک‌های مهم 	<p>در توسعه یک سرویس به دلیل مازولار کردن بخش‌ها باید فعالیت‌ها و سیاست‌های امنیتی در هر کدام از بخش‌ها به صورت مجزا اعمال شود؛ به طوری که در هر بخش مسائل امنیتی با درجه اهمیت بالاتر باید در اولویت قرار گیرد. زمان‌بندی فعالیت‌های امنیتی سرویس به شرح زیر است:</p> <ul style="list-style-type: none"> مروری بر مفاهیم اصلی امنیت در چرخه حیات سرویس‌های تحت وب تئیه 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 ساخت افزاری انتخاب رویکردها و روش‌های امن در پایگاه داده شناسایی و ارزیابی ریسک‌های مهم

ارائه شاخصهای امنیتی در چرخه حیات توسعه سامانه جویش‌گر بومی

<p>3. Assess Business Impact</p> <p>نحوه دار است:</p> <p>نمایه سازی از اهمیت سیستم سرویس از سرویس برای کدام بخش از سرویس در حفظ پایداری، دسترسی پذیری و شهرت سیستم سرویس از اهمیت بیشتری</p>	<p>2. Categorize the Information System</p> <p>طبقه بندی اجراء سیستم از نظر اهمیت امنیتی روی CIA (کم، متوسط، زیاد)</p>	<p>میزان اهمیت امنیتی مؤلفه ها بر اساس CIA به ترتیب زیر است:</p> <p>نمايه ساز:</p> <ul style="list-style-type: none"> پایگاه داده نمايه ساز بر اساس CIA بيشترین اهمیت را دارد (زياد). ماژول جستجو یا موتور بازيابی از لحاظ اهمیت در جايگاه دوم قرار می گيرد (متوسط). الگوريتمها، سياست های امنیتی، ساختمان داده ها و نرم افزارهای نمايه سازی در جايگاه بعدی قرار می گيرند (متوسط). پایگاه داده خوش گر نيز نسبت به اجزای دیگر خوش گر اهمیت بالاتری دارد (زياد). الگوريتمها، سياست های امنیتی و نرم افزارهای خوش گر در رتبه بعدی قرار می گيرند (متوسط). رتبه بند: الگوريتمها، سياست های امنیتی و نرم افزارهای رتبه بندی صفحات، بالاترین اهمیت را در اين مؤلفه دارند (زياد). <p>میزان اهمیت امنیتی مؤلفه ها بر اساس CIA¹ به ترتیب زیر است:</p> <p>سرديس:</p> <ul style="list-style-type: none"> پایگاه داده سرویس بر اساس CIA بيشترین اهمیت را دارد (زياد). ماژول جستجو (به عنوان مثال، در سرویس شبکه اجتماعی جستجوی افراد با ماژول جستجو انجام می شود) از لحاظ اهمیت در جايگاه دوم قرار می گيرد (متوسط). الگوريتمها، سياست های امنیتی، ساختمان داده ها و نرم افزارها در جايگاه بعدی قرار می گيرند (متوسط). در وب سرور نيز بر اساس نوع و میزان خدمت دهی باید ويزگي دسترسی پذيری را تأمین و تضمین کند (بالا). همچنان هنگام استفاده از سرور برنامه کاربردی باید ويزگي دسترسی پذيری نسبت به سایر روش ها تأمین شود (متوسط).
---	---	---

¹ Confidentiality-Integrity-Availability

دو فصل نامه علمی ترویجی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)

<p>4. Assess Privacy Impact</p> <p>مکان و نحوه ذخیره سازی اطلاعات خصوصی کاربران و درجه خصوصی بودنش چیست؟</p>	<p>از آنجا که هسته اصلی جویش گر با اطلاعات وبسایتها در ارتباط است و ارتباط کمتری با اطلاعات کاربران دارد، درجه اهمیت حريم خصوصی کاربران کمتر است. البته اگر سرویس‌های جویش گر به‌گونه‌ای باشد که کاربران اطلاعات خود را ثبت کنند انگاه باید به مسئله حريم خصوصی و امن‌کردن اطلاعات کاربران توجه جدی شود. به هر حال برای امن‌کردن و جلوگیری از نشت هر اطلاعاتی، نحوه ذخیره‌سازی اطلاعات در پایگاه باید بر اساس سیاست‌ها و قابلیت‌های زیر انجام شود:</p> <ul style="list-style-type: none"> • رمزگذاری فایل‌های داده برای برقراری محترمانگی داده‌ها؛ • ردگیری عامل انجام عملیات در پایگاه داده (نظرارت‌پذیری)؛ • اعتبارسنجی اندازه، قالب، بازه و نوع داده‌های ورودی؛ • بررسی هویت کاربران در ارتباط با ردگیری نظارتی و اجازه دسترسی به داده‌های خاص؛ • توجه به مسائل سازگاری اطلاعات ذخیره‌شده در پایگاه داده؛ • پشتیان‌گیری از داده‌ها و اطلاعات ذخیره‌شده برای افزایش دسترسی‌پذیری؛ • گسترش‌سازی و دانه‌بندی کردن منابع ذخیره‌سازی؛ • امن‌کردن ارتباطات با استفاده از پروتکل‌های امنیتی بین پایگاه داده و مازول‌های دیگر؛ • مدیریت قوی کلیدهای پایگاه داده‌ای؛ • انتخاب پایگاه داده مناسب با بعد و نوع داده‌های ذخیره شده هر سرویس.
<p>5. Ensure Secure Information System Development</p> <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 سرویس‌های طراحی شده است؛ زیرا این دو سطح جزء نخستین روزنه‌هایی هستند که مهاجم از طریق آن‌ها به هسته سرویس دسترسی می‌تواند پیدا کند. البته در این بخش، به سرورهای مهمی همانند وبسرور نیز می‌توان اشاره کرد.</p>

¹ Hardware Security Module

ارائه شاخصهای امنیتی در چرخه حیات توسعه سامانه جویش‌گر بومی

مرحله ۲ - توسعه و اکتساب		خرش‌گر - نمایه‌ساز-رتبه‌بند	سرویس‌های تحت وب
Accessibility, Integrity	1. Assess Risk to System	<p>شناخت نقاط ضعف در طراحی، محدودیت‌های پژوهش و تهدیدها</p> <p>مسلمان معماری جویش‌گر باید به صورت دوره‌ای بررسی شود تا مناسب با تهدیدات جدید افزونه‌های امنیتی به معماری اضافه شود. مهم‌ترین تهدیدهایی که هسته اصلی جویش‌گر را هدف قرار می‌دهد آسیب‌پذیری‌های تحت وب، پایگاه داده‌ای و حمله بهینه‌سازی جویش‌گر^۱ (SEO) است که باید به طور پیوسته راهکارهای امنیتی برای آن‌ها بررسی شوند.</p>	<p>معماری سرویس باید به صورت دوره‌ای بررسی شود تا مناسب با تهدیدات جدید افزونه‌های امنیتی به معماری اضافه شود. همچنین باید مدل سازی تهدید در این مرحله صورت گیرد.</p>
	2. Select and Document Security Controls	<p>تعیین کنترل‌های امنیتی و دسته‌بندی آن‌ها از نظر پایه‌بودن، اضافه و مکمل و سفارشی‌بودن. این کنترل‌های امنیتی چرا پیغامده و حضور باد اعمال شوند؟</p> <ul style="list-style-type: none"> • بهره‌گیری از الگوهای برتر برای کنترل‌های امنیتی؛ • کنترل‌های امنیتی برای سیاست‌های خرس، وب‌گاه‌های آلوده و حمله بهینه‌سازی جویش‌گر (SEO) • کنترل‌های امنیتی در هنگام نمایه‌سازی برای وب‌گاه‌های آلوده و حمله بهینه‌سازی جویش‌گر (SEO) • 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 برنامه کاربردی برای مقابله با حملات مرتبط با آن؛ • اعمال سیاست‌ها و کنترل‌های امنیتی متناسب با سرویس‌های طراحی شده. 	

¹ Search Engine Optimization

دو فصل نامه علمی ترویجی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)

<p>3. Design Security Architecture</p> <p>معماری امنیتی مشخص شود و ابزارهای کنترلی امنیتی پایه مشخص شود.</p>	<p>برای امن کردن معماری جویش گر باید مازول های آن در ساختار امنیتی DMZ^۱ در میان حفاظه ای داخلی و خارجی قرار گیرد تا سیاست های امنیتی مثل کنترل دسترسی، محرومانگی، صحبت داده و غیره به صورت سلسله مراتقی در آن اعمال شود. همچنین استفاده از رویکرد دفاع در عمق به منظور افزایش امنیت در بستر سرویس های جویش گر توصیه می شود.</p> <p>مهمنترین 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 رمز نگاری در سرویس هایی با ارزش اطلاعاتی بالا؛ • ارزیابی ضمانت امنیتی سرویس؛ • مستند سازی؛ • ارزیابی موارد پایه طراحی؛ • در نظر گرفتن حریم خصوصی در طراحی سرویس؛ • تهیی 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 گستردگی و جمع آوری فعالیت های مشکوک. 	<p>برای امن کردن معماری سرویس باید مازول های آن در ساختار امنیتی DMZ^۱ در میان حفاظه ای داخلی و خارجی قرار گیرد تا سیاست های امنیتی مثل کنترل دسترسی، محرومانگی، صحبت داده و غیره به صورت سلسله مراتقی در آن اعمال شود. همچنین استفاده از رویکرد دفاع در عمق به منظور افزایش امنیت در بستر سرویس های جویش گر توصیه می شود.</p> <p>مهمنترین 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 رمز نگاری در سرویس هایی با ارزش اطلاعاتی بالا؛ • ارزیابی ضمانت امنیتی سرویس؛ • مستند سازی؛ • ارزیابی موارد پایه طراحی؛ • در نظر گرفتن حریم خصوصی در طراحی سرویس؛ • تهیی 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 گستردگی و جمع آوری فعالیت های مشکوک.
--	---	---

¹ Demilitarized Military Zone

4. Engineer in Security and Develop Controls	فراهم کردن ابزارهای کنترلی اضافی و سفارشی شده باید مشخص شوند، پیانسیل جهت نسبت آسیب پذیری های محدودیت های شناخته شده	<p>برای امن کردن معماری جویش‌گر و سه مازول اصلی آن، علاوه بر کنترل های امنیتی پایه راه کارهای زیر را برای بهبود امنیت معماری می توان استفاده کرد:</p> <ul style="list-style-type: none"> استفاده از ساختارهای امن SOC¹ و NOC² برای نظارت و کنترل بیشتر مازول های جویش‌گر (HP Arc Sight)؛ پیاده سازی سورهای خزش‌گر، نمایه ساز و رتبه بند روی سخت افزارهای مجزا و ایزوله یا روی فناوری های مجازی Multi-Tenant این من استفاده از سیاست های امنیتی برای مبارزه با حمله بهینه سازی جویش‌گر (SEO) و وب گاه های آلوده در سطح خزش‌گر و نمایه ساز استفاده از ساختارهای امنیتی مثل هانی پات ها برای به دست آوردن اطلاعات بیشتر از مهاجمان و ارائه سناریوهای از پیش تعیین شده به مهاجم 	<p>برای امن کردن معماری سرویس، علاوه بر کنترل های امنیتی پایه می توان راه کارهای 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 سیاست های امنیتی استفاده از ساختارهای امنیتی برای به دست آوردن اطلاعات بیشتر از مهاجمان
5. Develop Security Documentation	اعزیزی اثوان حریم خصوصی با توجه به بلوغ سرویس های امنیتی، تکمیل طرح امنیتی	<p>از آنجا که جویش‌گر بیشتر با اطلاعات وب گاه ها در ارتباط هستند و فقط در زمان استفاده از سرویس های خاص ممکن است بر اساس اطلاعات کاربران جستجوها انجام شود. در این زمان نیاز است که سیاست های جلوگیری از نشت اطلاعات در جویش‌گر لحاظ شود که تا در زمان جستجوی وب گاه ها رد پای از کاربران به جای نماند. علاوه بر رعایت حریم خصوصی کاربران در زمان جستجو، جویش‌گر باید سیاست های امنیتی داشته باشد که از اطلاعات ذخیره شده کاربران در پایگاه داده نیز محافظت کند؛ این سیاست ها در قسمت Privacy Impact Assessment از مرحله یک چرخه حیات تشریح شده است.</p> <p>علاوه بر حریم خصوصی کاربران، جویش‌گرها باید حریم خصوصی وب گاه ها را نیز در نظر بگیرند. زیرا اگر یک جویش‌گر از سیاست های حفظ حریم خصوصی بهره نبرد، ممکن است، اطلاعاتی از وب گاه را در نتایج جستجو نشان دهد که مالک وب گاه راضی به نشان دادن آن به طور موقت نیست. بنابراین اعمال سیاست های امنیتی در سطح جویش‌گر برای نقض حریم خصوصی وب گاه ها نیاز است.</p>	<p>استفاده از ساختار و تنظیمات حریم خصوصی برای پیش گیری از آسیب های تحت سرویس؛ به روزرسانی، مرور و تکمیل سند حریم خصوصی کاربران در ضمن انتشار نسخه جدید سرویس جدید و قدیم جویش‌گر</p>

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 منظره</p>	<p>این بخش از فاز توسعه برای هر سه مؤلفه خرزش گر، نمایه‌ساز و رتبه‌بند همواره نیاز است و باید پس از توسعه نهایی مؤلفه‌ها آزمون‌های 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 خرزش گر:</p> <ul style="list-style-type: none"> • آزمایش حملات جلوگیری از سرویس؛ • آزمایش حملات تزریق کد به اسپایدرها؛ • سیاست‌های خرزش؛ • امنیت پایگاه داده‌ها؛ • ارزیابی فاکتورهای طراحی مثل پهنهای باند، توان عملیاتی و پردازشی سروورها و غیره • حمله بهینه‌سازی جویش‌گر(SEO) و وب‌گاه‌های آلوده؛ • آزمون نمایه‌ساز: • فاکتورهای ساختمان داده؛ • آزمایش و ارزیابی فاکتورهای طراحی؛ • امنیت پایگاه داده‌ها؛ • آزمایش پارامتر زمانی دوره بهروزرسانی نمایه‌ساز • آزمایش مازول مثبت جستجو و موتور بازیابی در برابر انواع حملات تحت وب و داخلی؛ • حمله بهینه‌سازی جویش‌گر(SEO) و وب‌گاه‌های آلوده • آزمون رتبه‌بند: • آزمایش و ارزیابی فاکتورهای طراحی • آزمایش و ارزیابی راهکارهای امنیتی مقابله با وب‌گاه‌های آلوده؛ • آزمایش راهکارهای امنیتی برای مقابله با حمله بهینه‌سازی جویش‌گر(SEO). 	<p>آزمون‌های زیر پس از توسعه نهایی مؤلفه‌های 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 (DoS¹)؛ • آزمایش حملات مرتبط با واسط کاربری جویش‌گر مانند بررسی نقاط ورودی؛ • بررسی امنیت پایگاه داده‌ها و مقاومت آن در برابر حملات شناخته شده؛ • آزمایش و ارزیابی فاکتورهای طراحی؛ • آزمایش پارامتر زمانی دوره بهروزرسانی؛ • آزمایش مازول های سرویس جویش‌گر در برابر انواع حملات تحت وب.
--	---	---

¹ Denial of Service

مرحله ۳ - پیاده‌سازی / ارزیابی	خرش‌گر - نمایه‌ساز - رتبه‌بند	سرویس‌های تحت وب
Authorizat ion	1. Create Detailed Plan for C&A تشکیل چنینیات صدورگواهی مدل محدودیت پروژه، محدوده آزمایش، سطح دقت و غیره در آن مشخصه هی شود.	<p>مسلمًاً مجوز و گواهی انجام یک کار برای مرحله پیاده‌سازی در صورتی برای جویش‌گر و مؤلفه‌های آن ارائه می‌شود که تمام محدودیت‌ها و آزمایش‌های امنیتی لازم برای مؤلفه‌های اصلی جویش‌گر در مرحله توسعه به درستی 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 خرس‌گر، نمایه‌ساز و رتبه‌بند ارائه شود؛ زیرا با وجود سند برنامه‌ریزی شده یکپارچگی اجزای جویش‌گر در مراحل بعدی به نحو بهتری انجام خواهد شد.</p>
	2. Integrate Security into Established Environments or Systems یکپارچه‌سازی سیستم‌های عملیاتی، تأییدکردن لیست کنترل‌های امنیتی، جایی جهت فعال‌سازی	<p>پس از اینکه مرحله توسعه برای سه مؤلفه اصلی تمام شد، فهرست سیاست‌های کنترلی و نظارتی امنیتی، تجزیه و تحلیل می‌شود و درنهایت این سیاست‌ها در مرحله بعد آزمایش و ارزیابی می‌شوند (فهرست کنترل‌های امنیتی شامل سیاست‌های خرس، سیاست‌های نمایه‌ساز، سیاست‌های رتبه‌بندی، سیاست‌های مربوط به مجوزدهی و کنترل‌های دسترسی در پایگاهداده‌ها و غیره می‌تواند باشد)؛</p>
3. Assess System Security ارزیابی امنیتی امنیتی اجرایی، بهزودرسانی طرح‌های امنیتی	<p>آزمایش بُعدهای امنیتی قبل از اعطاء مجوز، آزمایش‌های دوره‌ای و تأیید اثر بخشی کنترل</p> <p>آزمایش جعبه سیاه (آزمایش جعبه سیاه)</p> <p>تعیین آسیب‌پذیری‌ها و خطاهای نرم‌افزاری و سخت‌افزاری مربوط به مرحله توسعه برای بازگشت به ابتدای چرخه</p>	<ul style="list-style-type: none"> آزمایش بُعدهای 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 توصیه شده و ابزارهای امنیت در توسعه چرخه حیات)؛ تحلیل تمام توابع پروژه و API‌ها بهمنظور کاهش نقص‌های نرم‌افزاری امنیتی؛ استفاده از فایل‌های سرامد، کامپایلرهای جدید و ابزارهای پویش 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

دو فصل نامه علمی ترویجی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)

			مسلمانً 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 مژاول‌ها ارزیابی شود و مجوز نهایی درصورتی به سامانه مربوطه ارائه می‌شود که بتواند در برابر انواع آزمایش‌ها اینم باشد. برخی از جنبه‌های امنیتی که باید در این مرحله بررسی شود شامل محمانگی، حریم خصوصی، صحت داده‌ها، کنترل دسترسی، امنیت ارتباط و دسترسی‌پذیری است.	<ul style="list-style-type: none"> • تهیه مدلی جهت کنترل دسترسی افراد به سرویس‌های طراحی و توسعه‌یافته جویش‌گرهای بومی و ثبت رویدادها
	مرحله ۴ - نگهداری / اجرا	خوش‌گر - نمایه‌ساز - رتبه‌بند	سروریس‌های تحت وب	
Authentication, Robustness	1. Review Operational Readiness	<ul style="list-style-type: none"> - پیاده‌سازی سیاست‌های کلی برای پایداری و در دسترس‌بودن سامانه؛ - تعیین رویه‌ها و چارچوب‌های کاری برای تغییرات نرم‌افزاری و سخت‌افزاری در هر دوره از چرخه حیات؛ - بررسی آمادگی اجرایی برای توسعه سرویس‌های جویش‌گرهای بومی؛ - تحلیل پویا و تأیید بلاذرنگ سرویس با استفاده از ابزارهای پویشگر 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 ازدسترس خارج شدن سرویس. 		
	2. Perform Configuration Management	<p>(يون هر تغییر سخت افزاری و نرم افزاری می تواند بر این بخش شامل سه مؤلفه اصلی می شود؛ زیرا به مرور زمان با افزایش تعداد درخواست‌ها و کاربران یا به وجود آمدن تهدیدهای جدید نیاز است که در سخت‌افزار و نرم‌افزار مؤلفه‌های اصلی جویش‌گر تغییراتی اعمال شود.</p> <p>تغییرات سخت‌افزاری بیشتر به مسئله مقیاس‌پذیری سامانه برمی‌گردد و تغییرات نرم‌افزاری به مسائل موازی‌سازی فرایندها برای بهبود سرعت جستجوها و راه‌کارهای امنیتی مربوط به رتبه‌بندی برای مقابله با حمله بهینه‌سازی جویش‌گر (SEO) اشاره می‌کند. درواقع راه‌کارهای امنیتی رتبه‌بند باید بهطور دائمی در حال بهبود باشند.</p>	<p>با افزایش تعداد درخواست‌ها و کاربران یا به وجود آمدن تهدیدهای جدید نیاز است که در سخت‌افزار و نرم‌افزار مؤلفه‌های اصلی سرویس تغییراتی اعمال شود.</p>	

ارائه شاخصهای امنیتی در چرخه حیات توسعه سامانه جویش‌گر بومی

			<p>3. Conduct Continuous Monitoring</p> <p>ناظرات مداوم از اثربخشی کنترل امنیت در خود ارزیابی، مدیریت و صله، آزمایش امنیت، پیشگیری، مدیریت آنلاین و پروس، مدیریت و صله، آزمایش امنیت، از زیبایی و یا ممیزی</p>	<p>یک سامانه به دلیل وجود تهدیدهای جدید در طول زمان با تغییراتی همراه خواهد بود؛ بنابراین برای مقابله با تهدیدهایها و بهبود عملکرد امنیتی سامانه نیاز است که تهدیدهای و بهبود عملکرد امنیتی سامانه نیاز است که بهطور پیوسته از گام‌های زیر استفاده کرد:</p> <ul style="list-style-type: none"> • بهره‌گیری از ابزارهای نظارتی و کنترلی برای سطح خوش‌گر، نمایه‌ساز و رتبه‌بند برای جلوگیری از اثرات مخرب به سطوح دیگر؛ • استفاده از وصله‌های امنیتی برای پلتفرم سرورهای خوش‌گر، نمایه‌ساز و رتبه‌بند به‌طور دائمی؛ • بهره‌گیری از ضدبدافزارها و نرم‌افزارهای پالایش محتوا برای شناسایی وب‌گاه‌های آلوده در سطح مراحل خوش‌گر، نمایه‌ساز و رتبه‌بندی. 	<p>یک سامانه به دلیل وجود تهدیدهای جدید در طول زمان با تغییراتی همراه خواهد بود؛ بنابراین برای مقابله با تهدیدهایها و بهبود عملکرد امنیتی سرویس‌ها نیاز است که بهطور 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		خرش‌گر - نمایه‌ساز - رتبه‌بند		سرویس‌های تحت وب
Access Control, Authorization	1. Build and Execute Disposal or Transition Plan	طریق خاتمه یا انتقال سامانه	<p>پس از توسعه و پیدا‌سازی تمام مأذول‌های جویش‌گر نوبت به گزارش‌دهی و ارائه اطلاعات تکمیلی از روند کار است. بنابراین طرح جامع اطلاعاتی که نشان‌دهنده تمام‌شدن 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 درنهایت عملیات انتقال سامانه یا بخشی از آن صورت گیرد.</p>	<p>تشخیص مخاطبان اضطراری امنیت و تهیه طرح سرویس امنیت برای کدهای موروثی از دیگر گروههای سازمانی و کد شخص ثالث؛</p> <p>مستندسازی تمام و یا بخشی از اطلاعات پروژه با دلایل و مستندات کافی؛</p> <p>شناسایی، محاسبه ریسک‌های احتمالی و مدیریت ریسک‌ها؛</p> <p>حفظ و ذخیره اطلاعات حیاتی مانند طرح‌های امنیتی و نیازمندی‌های کنترل امنیت به‌طور منظم؛</p> <p>ساخت و اجرای طرح واگذاری / انتقال محصول جویش‌گرهای بومی.</p>	
	2. Ensure Information Preservation	الزامات قانونی، نمایه‌سازی اطلاعات و محل نگهداری آنها و خصوصیت‌شناختن (پایگاه داده‌ها)	<p>پایگاه داده‌ها علاوه بر امن‌بودن وضعیت دسترسی‌های فیزیکی و منطقی، باید زیرساخت امن نیز داشته باشند.</p> <p>برخی از الزاماتی که باعث امن‌شدن ذخیره‌سازی داده‌های هر مرحله می‌شود به شرح زیر است:</p> <ul style="list-style-type: none"> • اینمی 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 	<p>برخی از الزاماتی که باعث امن‌شدن ذخیره‌سازی داده‌های هر مرحله می‌شود به شرح زیر است:</p> <ul style="list-style-type: none"> • اینمی 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 	

دو فصل نامه علمی ترویجی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)

3. Sanitize Media	جلوگیری از دسترسی های غیرمجاز به اطلاعات بایگانی شده	<p>پس از اینکه اطلاعات حاصل از هر مرحله به صورت فیزیکی یا دیجیتال مستند شد و در محل های ذخیره سازی و پایگاه داده های مربوطه قرار گرفت، باید یکسری سیاست امنیتی اعمال کرد که هر کاربر یا مأذولی به اطلاعات نمایه شده دسترسی پیدا نکند.</p> <p>سیاست های کلی بدین صورت است:</p> <ul style="list-style-type: none"> • تصدیق اصالت و هویت شناسی کاربران داخلی و خارجی؛ • محدود کردن دسترسی های فیزیکی به منابع پایگاه داده ای و محل های ذخیره سازی اطلاعات مهم سرویس ها • ارائه یک شمای کلی از اطلاعات و دادن سطوح دسترسی عمومی به کاربران مصرف کننده سرویس های جویش گرهای بومی به طوری که امنیت اطلاعات به مخاطره نیفتند. 	<p>مستندسازی اطلاعات حاصل از هر مرحله به صورت فیزیکی یا دیجیتالی و قرار گرفتن آنها در محل های ذخیره سازی و پایگاه داده های مربوطه، باید با اعمال سیاست های امنیتی مانع دسترسی هر کاربر یا مأذولی به اطلاعات مهم شود. سیاست های کلی بدین صورت است:</p> <ul style="list-style-type: none"> • تصدیق اصالت و هویت شناسی کاربران داخلی و خارجی در استفاده از انواع سرویس های جویش گرهای بومی؛ • محدود کردن دسترسی های فیزیکی به منابع پایگاه داده ای و محل های ذخیره سازی اطلاعات مهم سرویس ها • ارائه یک شمای کلی از اطلاعات و دادن سطوح دسترسی عمومی به کاربران مصرف کننده سرویس های جویش گرهای بومی به طوری که امنیت اطلاعات به مخاطره نیفتند.
4. Dispose of Hardware and Software	پرسی و ضمیمه فروش، اهدا یا امحای ساخت افزار و نرم افزار سامانه افزا	<p>پیاده سازی سیاست های مربوط به امحای اطلاعات در سامانه توسعه یافته اعمال سیاست های انتقال نرم افزار و سخت افزار در سامانه پیاده سازی شده</p> <ul style="list-style-type: none"> • پیاده سازی سیاست های مربوط به امحای اطلاعات سرویس های قبلی 	<ul style="list-style-type: none"> • پیاده سازی سیاست های مربوط به امحای اطلاعات سرویس های قبلی
5. Close System	خاتمه سامانه با مجوز نهایی	<p>بایگانی و طبقه بندی کردن تمام اطلاعات سامانه ارائه مجوز شروع به کار سامانه توسعه یافته</p> <ul style="list-style-type: none"> • باسخ گویی مناسب به گزارش های آسیب پذیری ها و تهدید های سرویس توانایی پیاده سازی طرح پاسخ گویی رویداد به منظور حفاظت از مشتریان در برابر آسیب پذیری های حریم خصوصی و امنیت سرویس 	<ul style="list-style-type: none"> • بایگانی و طبقه بندی کردن تمام اطلاعات سامانه • ارائه مجوز شروع به کار سامانه توسعه یافته • پاسخ گویی مناسب به گزارش های آسیب پذیری ها و تهدید های سرویس • توانایی پیاده سازی طرح پاسخ گویی رویداد به منظور حفاظت از مشتریان در برابر آسیب پذیری های حریم خصوصی و امنیت سرویس

۵- نتیجه گیری

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

همانطور که اشاره شد برای ایمن سازی سامانه های اطلاعاتی و سرویس های تحت وب می باشد، ابتدا به شناسایی اصول و ابزارهای کنترل امنیتی و چارچوب ها و الگوهای امنیتی آن پرداخت، این ابزارهای کنترلی، عملیاتی، فنی و یا مدیریتی می توانند باشند. مرحله بعدی، استخراج اصول اولیه ایمن سازی سرویس، مشتمل بر شناسایی، تشخیص و مدل سازی تهدید ها در خصوص 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 fundamentals 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.

سه بعدی (۱) ارائه شده بازخوردهای عملیاتی مؤلفه های 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.



nasrin taj فارغ التحصيل کارشناسی ارشد مهندسی فناوری اطلاعات گرایش مخابرات امن در سال ۸۸ از دانشگاه علم و صنعت ایران و پژوهشگر مرکز تحقیقات مخابرات امیرکبیر، ۹۵/۲/۲۳

دو فصل نامه علمی ترویجی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)

ایران است. زمینه‌های پژوهشی ایشان امنیت شبکه و فناوری اطلاعات، امنیت جویشگر 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 دکتراخود 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 سرکندي 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 مديا روی اينترنت، جريان‌سازی ويديو نظير به نظير، امنیت سامانه‌های مبتنی بر شهرت و طراحی امن معماري شبکه است.

افتا
من روی
علی ترویجی
علمی