

Preventive Security Architecture of Computer Systems

Yasaman Pouladzadeh¹, Nasser Modiri^{2*}

1.MSc Student, Department of Computer Engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran.

yasamanpouladzadeh@yahoo.com

2.Assistant professor, Department of Computer Engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran.

(Corresponding Author)

Nassermodiri@yahoo.com

Abstract

Introduction: Despite the significant growth of theoretical teaching methods and the development of teaching aids, there are still many problems in the education system, especially in universities. In similar conditions, the challenges of education and problems after graduation in the fields of science, technology, engineering, and mathematics (STEM) are more obvious. Although today there is a large amount of research on how to deal with the issues related to the quality of education, these methods were generally not successful and most of those who finish a degree in the university, are usually unprepared. They are not required to enter the labor market. In this article, a hybrid method called HEAL is introduced, which is especially effective in STEM education. This proposed approach can be considered a combination of teaching and learning and is a transformation that leads a person from being a mere student to becoming an active learner. The main idea of this approach is based on the fact that in university, a student is expected to be a researcher of knowledge, unlike a student who acquires knowledge through education.

Method: hybrid education and learning (HEAL) is a skill-based, time-based method of instruction that combines face-to-face learning and virtual learning. Proficiency-oriented, time-based education provides a model in which students who fail to earn a passing grade or complete a course during a semester are given time to demonstrate competency.

Findings: The basic philosophy of HEAL is to prove the skills and abilities of students, with an approach similar to the driver's license test. This means that if the test is failed, the learner is given an opportunity to improve and try another way to demonstrate mastery. The financial capability of universities is the most important factor in making this approach operational. However, this financial burden is negligible compared to course repetition, delayed graduation, and sometimes even more academic failure. HEAL removes the fear of exams and failure and increases the love of learning.

Discussion: The combination of face-to-face and virtual learning can become a wider trend in the university. While we must remember the fact that nothing can replace face-to-face training and the need for student-faculty interaction. In this research, a method for teaching in universities was discussed, in which time-based and competency-based education are combined with face-to-face and virtual learning, which can be a successful approach with the aim of reducing academic retention.

Keywords: cyber - defense, preventive, security, organization.

معماری امنیت پیشگیرانه سیستم‌های کامپیوتری

دوره اول، زمستان ۱۳۹۹
شماره دوم، صص: ۷ - ۱۵

تاریخ دریافت: ۱۳۹۹/۰۹/۰۱
تاریخ پذیرش: ۱۳۹۹/۱۰/۱۵

یاسمن پولادزاده^۱، ناصر مدیری^{۲*}

۱. کارشناسی ارشد، گروه مهندسی کامپیوتر، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران.

yasamanpouladzadeh@yahoo.com

۲. استادیار، گروه مهندسی کامپیوتر، واحد زنجان، دانشگاه آزاد اسلامی، زنجان، ایران. (نویسنده مسئول) Nassermodiri@yahoo.com

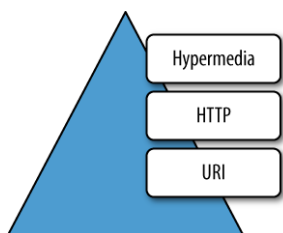
چکیده: مقابله با تهدیدات سایبری به معنی حفاظت از مالکیت مادی و معنوی اطلاعات در تمامی حوزه‌ها و جلوگیری از سوءاستفاده است. بنابراین حفاظت از اطلاعات در برابر این تهدیدات، بدون آنکه اختلالی در رشد و توسعه ایجاد شود، امری ضروری و مهم است. در حال حاضر این موضوع تبدیل به یک مسئله مهم شده، طوری که امروزه مقابله با تهدیدات سایبری جدی‌ترین چالش برای دولت‌ها محسوب می‌شود. این حوزه رویکردهای متعددی برای تأمین امنیت سایبری دارد، یکی از این رویکردها دفاع پیشگیرانه است که سبب حفاظت از اطلاعات سازمان می‌شود. این مقاله مجموعه‌ای از معماری‌های مرجع و الگوی‌های پرکاربرد در امنیت سایبری را بررسی و بر اساس بهترین فعالیت‌های هر مدل، الگویی نوین ارائه می‌کند. چهارچوب‌ها و استانداردهای ارزیابی شده شامل چهارچوب NIST و استاندارد ISO 27000 و CERT هستند. مدل پیشگیری یک روش مداخله‌ای برای احتمال افتادن به موقع ریسک‌های شناخته شده است. مدل پیشنهادی شامل معماری در چهار سطح، فازهای پیاده‌سازی و اجرای مدل است، در معماری پیشنهادی سرویس‌ها، لایه‌ها و برنامه‌ها تشریح شده و در متدولوژی پیشنهادی فازها و فرایندهای عملیات مطرح گردیده است.

واژه‌های کلیدی: پدافند سایبری، پیشگیرانه، امنیت، سازمان، الگو، ساختارسازی.

۱. مقدمه

ود [۳].

شکل ۲ طرح لئونارد ریچاردسون است که بر اساس میزان سازگاری با REST



شکل ۲: مدل ریچاردسون

، آن‌ها را به چهار دسته تقسیم کرده است [۴].

ریچاردسون از سه عامل برای تصمیم‌گیری در مورد بلوغ یک سرویس یعنی URI، HTTP Methods و HATEOAS (Hypermedia) استفاده کرده است.

سطح صفر بلوغ از هیچ‌یک از قابلیت‌های URI، HTTP و HATEOAS استفاده نمی‌کند. سرویس‌های این سطح یک URI واحد دارند و از یک روش HTTP واحد (معمولاً POST) استفاده می‌کنند.

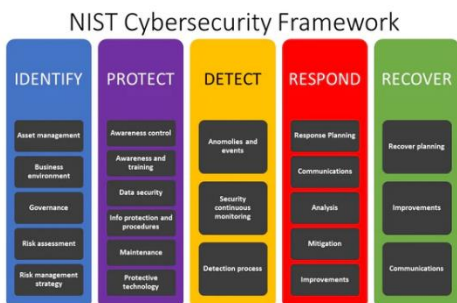
سطح اول باعث استفاده از URI‌ها از روش‌های HTTP و HATEOAS می‌شود. این سرویس‌ها بسیاری از URI‌ها را استخدام می‌کنند اما فقط یک فعل HTTP دارند.

سطح دو باعث می‌شود URI‌ها و HTTP از URI، HTTP Methods و HATEOAS خارج شوند. خدمات سطح دو، میزان منابع بیشتری با آدرس URI است. سطح دو مورد مناسبی برای استفاده از اصول REST است که طرفدار استفاده از افعال مختلف بر اساس روش‌های درخواست HTTP هستند و سیستم می‌تواند دارای چندین منبع باشد.

سطح سه از هر سه URI، HTTP و HATEOAS استفاده می‌کند. این بالغ‌ترین سطح مدل ریچاردسون است که قابلیت کشف پاسخ‌ها را با استفاده از HATEOAS آسان می‌کند.

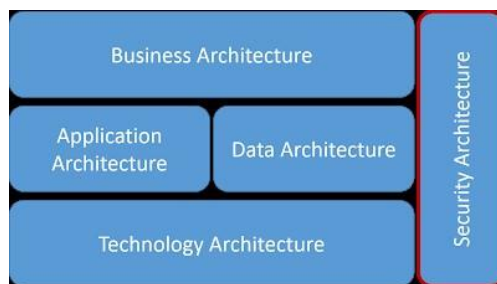
بعد از مدل ریچاردسون چهارچوب NIST مطرح شد. اولین نسخه چارچوب امنیت سایبری به منظور ارائه راهنمایی به سازمان‌های خواهان تقویت دفاع امنیت سایبری، انتشار یافت. در حالی که اکثریت قریب به اتفاق سازمان‌ها به اهمیت تقویت دفاع امنیت سایبری پی برده‌اند، اما این تلاش مشترک در جهت بهبود امنیت سایبری در تمامی سازمان‌ها و

شکل ۳: چارچوب امنیت سایبری در NIST



۲. پیشینه تحقیق

در این مقاله به مطالعه دو کار که شامل کار لئونارد ریچاردسون و مهم‌ترین مدل مرجع برای معماری امن سیستم‌ها که مدل NIST می‌باشد، پرداخته شده است. لئونارد ریچاردسون صد طرح مختلف وب سرویس را تجزیه و تحلیل کرد و بر اساس میزان سازگاری با REST، آن‌ها را به چهار دسته تقسیم کرد. این مدل از تقسیم خدمات REST



شکل ۱: معماری مرجع امنیت سایبری (SRA)

مهم‌ترین مدل مرجع برای معماری امن سیستم‌های کامپیوتری، مدل مرجع NIST می‌باشد که شامل ۵ مرحله است.

۱. مشخص نمودن اهداف: قبل از فکر کردن در مورد چرایی و چگونگی پیاده‌سازی NIST، هدف از این پیاده‌سازی باید مشخص باشد.
۲. تهیه یک پروفایل دقیق: گام بعدی، اجرای آزمایشی آن Framework به صورت تخصصی تر و برای پاسخگویی به نیازهای خاص سازمان می‌باشد.

۳. ارزیابی موقعیت فعلی: بعد از مراحل بالا خیلی مهم است که ارزیابی ریسک به صورت دقیق انجام شود، به طوری که می‌توان حالتی خاص را ایجاد نمود.

۴. آنالیز اختلاف بین نتایج و شناسایی اقدامات ضروری: با مطلع بودن از خطرات امنیت سایبری و تأثیرات تجاری بالقوه برای سازمان، می‌توان فاصله میان نتایج را آنالیز نمود.

۵. پیاده‌سازی یک طرح عملیاتی: با یک تصویر واضح از صحت دفاع امنیتی سایبری فعلی، مجموعه‌ای از اهداف سازمانی، تجزیه و تحلیل جامع فاصله میان نتایج واقعی و نتایج مورد انتظار و مجموعه‌ای از اقدامات اصلاحی، نهایتاً منجر به پیاده‌سازی NIST CSF به صورت مطلوب خواهد شد [۱] [۶].

سطح عملیاتی	تدوین برنامه تست نفوذ شبکه و نرم افزارها	مستندسازی فعالیت‌های پدافند غیرعامل سایبری	چک لیست اپراتورها
-------------	---	--	----------------------

مدل پیشگیرانه پدافند غیرعامل سیستم‌های کامپیوتری دارای ۷ لایه پایه‌ای و بنیادی (لایه زیرساخت، لایه سرویس، لایه محتوا، لایه کاربر، لایه امنیت، لایه مدیریت و تنظیم مقررات، لایه جداسازی مدیریت و تنظیم مقررات) و سخت‌افزارهای لازم برای فعال کردن عملکرد شبکه، کتابخانه‌ای از اطلاعات، زنجیره توزیع محتوا و... می‌باشد.

روش‌های مصون‌سازی سایبری شامل دفاع به روش خطی، دفاع بر اساس زون‌بندی، دفاع مبتنی بر اعتماد (اطمینان) به اطلاعات، دفاع در عمق (دفاع لایه به لایه) می‌باشد که با استفاده از امتیازبندی حملات، بخش‌بندی و منطقه‌بندی حملات مخرب استفاده می‌شود.

تعیین نوع رویکرد در دفاع سایبری نقش بسیار مهمی دارد که شامل رویکرد واکنش‌گرایانه، پیش‌کنش‌گرایانه، پیش‌بینی‌گرایانه، پیش‌دستانه می‌باشد.

نوع اقدامات سایبری با توجه به طبقه‌بندی زیرساخت به ۳ دسته اصلی تقسیم می‌شوند که شامل مصون‌سازی، استحکام‌بخشی، ایمن‌سازی می‌باشد.

هدف از تشخیص نفوذ نمایش، بررسی و ارائه گزارش از فعالیت شبکه است. نحوه کار سیستم‌های تشخیص در حوزه سایبر این صورت است که مانند یک ابزار شبکه اگر نشانه‌هایی از یک حمله یا رفتار مشکوک را متوجه شوند، ترافیک شبکه را مانیتور کرده و مدیر شبکه را مطلع می‌سازند، از مطرح‌ترین سیستم‌های تشخیص در حوزه سایبری می‌توان سیستم تشخیص نفوذ (IDS)، سیستم همبسته‌ساز رویدادها (IPS)، سیستم تله عسل (Honey pot) را نام برد [۵].

۴. معماری پیشگیرانه

مدل پیشگیرانه دارای ۴ رویکرد مؤلفه‌ای است که هر رویکرد دارای محیط‌های عملیاتی، از نوع مهم، حساس و حیاتی است و معماری پیشگیرانه شامل مقاوم‌سازی، استحکام‌بخشی، جداسازی و مصون‌سازی در چهار سطح شامل سطوح راهبردی تاکتیکی تکنیکی و عملیاتی می‌باشد که در شکل زیر مشاهده می‌کنید:



همچنین تطبیق و پیاده‌سازی این چارچوب، در عمل کار بسیار دشواری است [۱].

شکل ۳ چارچوب امنیت سایبری در NIST را نشان می‌دهد که به منظور ارائه راهنمایی به سازمان‌های خواهان تقویت دفاع امنیت سایبری، انتشاریافت.

۳. اجرای نمودن مدل پیشگیرانه

پیشگیری یک روش مداخله‌ای برای احتمال افتادن به موقع ریسک‌های شناخته‌شده است این مداخله دارای سطوح زیر می‌باشد. جهت اجرایی کردن مدل پیشگیرانه باید تعدادی برنامه داشته باشیم که هر برنامه تبدیل به فعالیت می‌شود و در ادامه هر فعالیت تبدیل به اقدامات می‌شود که در جدول (۱) می‌توان نمای از برنامه‌ها، فعالیت‌ها و اقدامات را مشاهده کرد:

جدول ۱: نمایی از برنامه‌ها، فعالیت‌ها و اقدامات

سطوح پیشگیرانه	برنامه‌ها	فعالیت‌ها	اقدامات
سطح راهبردی	شناسایی مقررات و جرایم در حوزه سایبری	تدوین فعالیت‌های سایبری	تدوین اقدامات پیشگیرانه سایبری
سطح تاکتیکی	شناسایی ۵ مرحله شناسایی NIST	شناسایی فعالیت‌های تهدیدات سایبری	اقدامات پیشگیرانه ایمن‌سازی بانک اطلاعاتی
سطح تکنیکی	شناسایی تداوم کسب و کار	فعالیت‌های فرآیند و مسئولیت‌ها در صورت هک سامانه	مستندسازی اقدامات پیشگیرانه فعالیت‌های پدافند غیرعامل سایبری
سطح تکنیکی	شناسایی مأموریت‌ها	مستندسازی فعالیت‌های اقدامات پیشگیرانه	تدوین اقدامات پیشگیرانه روش کار سایبری
سطح تکنیکی	شناسایی شاخص‌های کلی	فعالیت‌های فرآیند و مسئولیت‌ها در صورت ایجاد مشکل بر روی سامانه	بررسی و به روزرسانی قوانین و مقررات
سطح تکنیکی	شناسایی استراتژی تسلط سایبری	مستندسازی فعالیت‌های پدافند غیرعامل سایبری	مستندسازی و کنترل کلاس‌بندی اطلاعات
سطح تکنیکی	شناسایی ریسک‌های سایبری	مستندسازی فعالیت‌های اقدامات پیشگیرانه سایبری	تدوین فرآیند و مسئولیت‌ها در روش تعریف نیازمندی‌ها

شکل ۴: مدل معماری پیشگیرانه

۱.۴. سطح راهبردی

تعیین خطوط کلی رسالت سازمان در بلند مدت

قوانین و مقررات جمهوری اسلامی ایران	رویکرد کشور ما در حیطه مدیریت داخلی اینترنت، مبتنی بر قانونگذاری ملی است. طبق این قانون به موازات حق دسترسی آزاد به اطلاعات، بر رعایت حقوق داخلی در موضوعات اجتماعی، فرهنگی و فنی کشور تأکید شده است.
NIST	مهم‌ترین مدل مرجع برای معماری امن سیستم‌های کامپیوتری که شامل ۵ مرحله است.
CERT	تیم اصلی پاسخ‌گویی اضطراری کامپیوتر است. که همانند انسان برای آنتی‌ویروس عمل می‌کند.
SANS	شرکت SANS یکی از شرکت‌های قدرتمند در حوزه امنیت اطلاعات و یکی از بزرگترین و حرفه‌ای‌ترین تولید کننده آموزش‌های امنیت، تست نفوذ، جرم‌شناسی است.
FIRST	مجمع جهانی تیم‌های واکنش حوادث و امنیت است. با هدف تقویت همکاری و هماهنگی در جلوگیری از بروز حوادث، تحریک سریع واکنش در برابر حوادث و ترویج اشتراک اطلاعات بین اعضا و جامعه به طور کلی است.
NVD	در واقع مخزن داده‌های مربوط به آسیب پذیری‌های سیستم عامل‌ها است که به جهت مدیریت ریسک و امنیت دسته‌بندی می‌شوند.
SRA-CRA	آنالیز ریسک هزینه و تحلیل ریسک برنامه زمانبندی
جرایم	با توجه به تنوع و گستردگی استفاده از فضای مجازی، جرائم مرتبط با آن‌ها نیز از عناوین و موضوعات متعددی تشکیل شده و از تنوع و فراوانی بالایی برخوردار هستند.
فتا	فضای تولید و تبادل اطلاعات می‌باشد. که از وظایف این سازمان می‌توان به ایجاد امنیت و کاهش مخاطرات برای فعالیت‌های علمی، اقتصادی، اجتماعی در جامعه اطلاعاتی اشاره کرد.
ماهر	مرکز امداد و هماهنگی رایانه‌ای است. اهداف این سازمان شامل ایجاد یک نقطه کانونی در سطح وزارت ارتباطات و فناوری اطلاعات می‌باشد.
افتا	امنیت فضای تبادل اطلاعات است. تدوین راهبردها، نظارت بر حسن اجرای بخشنامه‌ها، دستورالعمل‌ها از مأموریت‌های افتا است.

جدول ۲: بررسی سطح راهبردی

۲.۴. سطح تاکتیکی

فعالیت‌ها برای رسیدن به اهداف میانی سازمان

تداوم کسب و کار	یک فرایند مدیریت جامع برای شناسایی تهدیدات احتمالی برای یک سازمان و تأثیرات عملیاتی این تهدیدات است.
تداوم مأموریت	کنترل و بررسی عملکردها بر اساس سیاست و اهداف تداوم تجارت، ارائه نتایج برای بررسی به مدیریت، بررسی اقدامات اصلاحی براساس نتایج بررسی مدیریت و ارزیابی مجدد.
SRS,DRP	هنگامی که برنامه‌های بازیابی حوادث به درستی طراحی و اجرا می‌شوند، امکان بازیابی کارآمد سیستم‌های حیاتی را فراهم می‌کند و به سازمان کمک می‌کند تا از آسیب بیشتر به عملیات مهم مأموریت جلوگیری کند.
سناریو non CIA	شناسایی اطلاعات و دارایی‌های مربوطه، به علاوه تهدیدات احتمالی، تصمیم‌گیری در مورد چگونگی رفع یا درمان خطرات
آستانه تحمل درد سایبری	مقداری که می‌توانیم با تهدیدهای سایبری سازگار باشیم.
NIST	مشخص کردن اهداف، تهیه یک پروفایل دقیق
NOC	مراکز عملیاتی شبکه که امروزه یک سرویس کاملاً متداول هستند و معمولاً براساس امکاناتی با صفحه نمایش بزرگ یا دیوارهای ویدئویی با ایستگاه‌های کاری برای اپراتورها و تحلیلگران، اتاق جلسات و...
SOC	مرکز عملیات امنیت اطلاعات مکانی است که در آن سیستم‌های اطلاعاتی شرکت کنترل، ارزیابی و دفاع می‌شوند.
CERT	تیم اصلی پاسخ‌گویی اضطراری کامپیوتر است.
رابطه بین NOC, SOC	انعطاف پذیری و به حداکثر رساندن دسترسی و کاهش قابل توجه خطر اطمینان برای شرکت و مشتریان در مورد ایمن نگه داشتن اطلاعات.
تست نفوذ	یک حمله سایبری شبیه‌سازی شده مجاز بر روی سیستم رایانه‌ای است که برای ارزیابی امنیت سیستم انجام می‌شود.
روش رزمایش سایبری	به منظور تعیین میزان آمادگی جهت حفاظت از دارایی‌ها و سامانه‌ها در قبال حملات، تمرین تصمیم‌گیری مدیریتی پاسخگو و...
روش دفاع passive	استتار، اختفاء، پوشش، فری، تفرقه و پراکندگی، مقاومت‌سازی و استحکامات اعلام خبر.
ستون‌های امنیتی	امنیت سایبری خصوصاً برای سازمان‌ها و کسب‌وکارهای امروزی اهمیت بالایی دارد و برای رسیدن به بهترین پیکربندی، باید ستون‌های اصلی آن را بشناسیم که شامل: فناوری، مدیریت و نظارت بر ساختار IT، آگاهی نیروی انسانی، اهمیت بسیار بالای فاکتور انسانی است.

Blue,Red,White Team	تیم‌های قرمز و آبی نقش مهمی در دفاع در برابر حملات پیشرفته سایبری دارند که ارتباطات تجاری، اطلاعات حساس مشتری یا اسرار تجاری را تهدید می‌کند. تیم سفید تیمی که نظارت بر مسابقات دفاع سایبری و قضاوت این رویداد را بر عهده دارد.
Cyber Defenders	برنامه‌های آزمایشی و مشارکتی در صنعت را ارائه می‌دهد که برای ارائه دروازه ورود به مشاغل امنیت سایبری ارائه شده‌است.
خودارزیایی سایبری	دارای اطلاعات زمینه‌ای در مورد امنیت سایبری است و گزینه‌های مختلفی را برای فرآیندها و سیستم‌های تجاری ارائه می‌کند.
اقدامات ضد تقلب	از این اقدامات می‌توان برای تقویت امنیت و اطمینان از عملکرد آنلاین مجموعه استفاده کرد که شامل شناسایی دستگاه‌های مورد استفاده در وب سایت و... است.
KFI	شاخص‌های اصلی کلاهبرداری که رویکرد جدیدی برای راه اندازی و استفاده از شاخص‌های مؤثر تقلب است.
UAM	ابزارهای نرم افزاری هستند که رفتار کاربر نهایی را در دستگاه‌ها، شبکه‌ها و سایر منابع IT متعلق به شرکت کنترل و ردیابی می‌کنند.
Insider Theread	تهدیدات داخلی، شامل خرابکاری، سرقت، جاسوسی، کلاهبرداری و مزیت‌های رقابتی اغلب از طریق سوءاستفاده از حقوق دسترسی، و سوءاستفاده از وسایل فیزیکی انجام می‌شود.
Kali	اصلی‌ترین ابزار مورد نیاز برای یک هکر یا متخصص امنیتی است و مجموعه‌ای عظیم از انواع ابزارهای تست امنیتی در شبکه اینترنت است.
Wire Shark	نرم‌افزار آنالیز پروتکل‌های شبکه می‌باشد و از قابلیت‌های مهم آن خواندن و نوشتن در فرمت‌های بسیار متنوع می‌باشد.
Owasp zap	یک اسکنر امنیتی برنامه وب منبع باز است. این برنامه در نظر گرفته شده‌است که توسط افراد تازه وارد در زمینه امنیت برنامه و همچنین تست‌های نفوذ حرفه ای مورد استفاده قرار می‌گیرد.

جدول ۴: بررسی سطح تکنیکی

۴.۴. سطح عملیاتی

فعالیت‌ها و گام‌های ویژه جهت رسیدن به اهداف.

ITIL	این یک رویکرد بسیار گسترده و قابل قبول در مدیریت خدمات فناوری اطلاعات است. هدف اصلی بهبود نحوه ارائه و پشتیبانی IT از خدمات با ارزش تجاری است.
------	--

Threat Management	مدیریت تهدیدات سایبری (CTM) یک برنامه مدیریت پیشرفته است که امکان شناسایی زود هنگام تهدیدها فراهم می‌کند.
Thered modling	مدل‌سازی تهدید عملی است برای شناسایی و اولویت بندی تهدیدات احتمالی و تخفیف‌های امنیتی
STRIDE	مراحل مختلف حمله را که از مدل Cyber Kill Chain مشتق شده‌است، توصیف می‌کند و سپس وظایف اصلی هر مرحله را نشان می‌دهد. در آخر لیستی از TTP متداول را که برای هر کار استفاده می‌شود، توصیف می‌کند.
DREAD	بخشی از سیستم برای ارزیابی ریسک تهدیدهای امنیتی رایانه است. و شامل آسیب، قابلیت تولید مجدد، بهره‌برداری، کاربران تحت تأثیر، قابلیت کشف است.
Thread Intelligence	اطلاعاتی است که یک سازمان برای درک تهدیداتی که سازمان دارد یا در حال حاضر هدف آن است، استفاده می‌کند.
ATP&TTP	دسته‌ای از راه‌حل‌های امنیتی که در برابر بدافزار پیچیده یا حملات مبتنی بر هک با هدف قراردادن داده‌های حساس دفاع می‌کنند.
ATT&CK	لیستی ساختاری از رفتارهای شناخته شده مهاجم است که در تاکتیک‌ها و تکنیک‌ها گردآوری شده و در تعداد انگشت‌شماری ماتریس و همچنین از طریق STIX / TAXII بیان شده‌است.
فریب سایبری	مکانیسم‌های کنترل دسترسی سیستم عامل‌های امن پنهان است.

جدول ۳: بررسی سطح تاکتیکی

۳.۴. سطح تکنیکی

شامل تکنیک کارهای قبل می‌باشد.

Cyber dominance strategy	سلطه سایبری تهاجمی استراتژیک از سوگیری سوءاستفاده‌های دشمن با ترکیبی از انفجار اطلاعات و دستکاری سوءاستفاده می‌کند.
Cyber range	یک محیط مجازی است که شرکت‌ها می‌توانند از آن برای آموزش جنگ سایبری و توسعه نرم‌افزار استفاده کنند.
اخلاق سایبر	به کد رفتار مسئولانه در اینترنت اشاره دارد.
CSC	رمزگذار امن سایبری خطر امنیت نرم افزار بسیار زیاد است و با این وجود بسیاری از تیم‌های توسعه دهنده تنها پس از تهیه کد و آماده سازی نرم افزار برای تحویل، با امنیت نرم‌افزار سر و کار دارند.
Cwss	مکانیسمی را برای اولویت‌بندی نقاط ضعف نرم‌افزار به روشی ثابت، انعطاف پذیر و باز فراهم می‌کند.

می تواند برای شناسایی تهدیدها، حملات، آسیب پذیریها و اقدامات متقابل کمک کند.	
Threat Hunting	شکار تهدید سایبری یک فعالیت فعال در زمینه دفاع سایبری است. این فرایند جستجوی فعالانه و تکراری از طریق شبکه ها برای شناسایی و جداسازی تهدیدات پیشرفته است.

جدول ۵: بررسی سطح عملیاتی

در ادامه رویکرد اجرایی براساس شکل ۵ معرفی می شود:

ITSM	مدیریت خدمات فناوری اطلاعات به این سادگی است که تیم های IT با ارائه خدمات نهایی به مشتریان خدمات را مدیریت می کنند.
ISMS	سیستم مدیریت امنیت اطلاعات مجموعه ای از سیاست ها و رویه ها برای مدیریت سیستماتیک داده های حساس سازمان است. هدف آن به حداقل رساندن ریسک و اطمینان از تداوم تجارت با محدود کردن فعالانه تأثیر نقض امنیت است.
19 cloud Security Cases	۱۹ مورد مهم برای امنیت cloud مطرح می شود.
آگاهی موقعیتی	به معنی آگاهی محور است و شامل تجزیه و تحلیل، ارزیابی ریسک سازمانی، بررسی سطح شرکت یا روند کارکنان می باشد.
مدیریت موضوع SDL	یکی از عناصر اصلی چرخه زندگی توسعه امنیت مایکروسافت است. این یک تکنیک مهندسی است که

شکل ۵: ارائه رویکرد اجرایی



در ابتدا باید به شناسایی دارایی ها شامل اطلاعات، مراکز، شبکه ها و تجهیزات سایبری و تعیین سطح اهمیت دارایی ها و شناسایی آسیب پذیری بپردازیم و بعد راهکاری به منظور کاهش آسیب پذیری ها و مقابله با تهدیدات مربوطه متناسب با سطح اهمیت آن ها ارائه دهیم و در پایان به پیاده سازی و اجرای راهکارهای ارائه شده بپردازیم که این مراحل در شکل (۶) ارائه شده است.

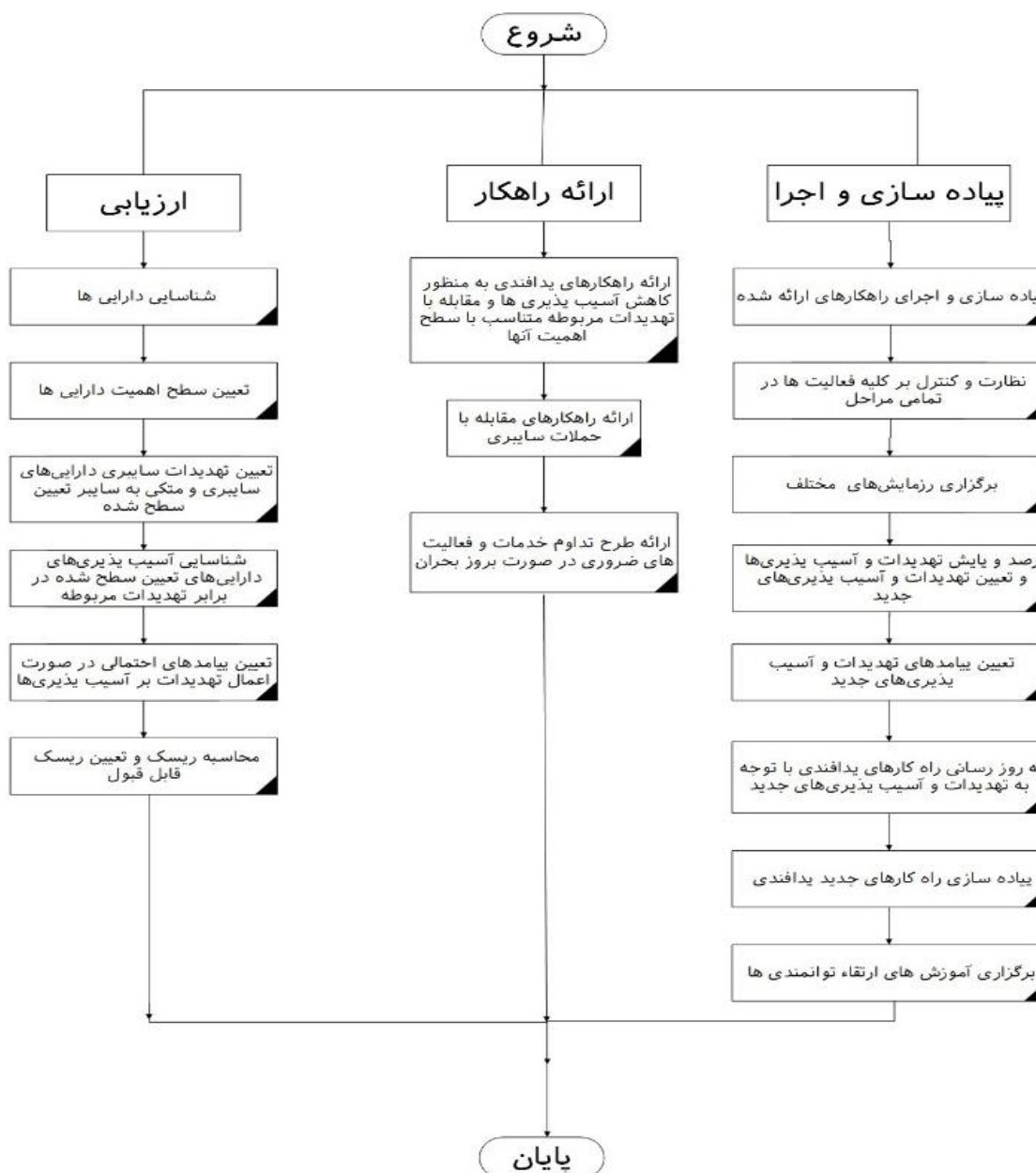
جهت اجرای مدل پیشگیرانه پدافند غیرعامل سیستم های کامپیوتری، برنامه اجرای آن شامل ۳ مرحله می باشد:

- ارزیابی
- ارائه راهکار
- پیاده سازی و اجرا

۵. نتیجه‌گیری

مرجع است، و با تحلیل رویکرد و ساختار آن‌ها در ارائه یک مدل پیشگیرانه، معماری پیشنهادی این مطالعه که شامل ۴ سطح، ۷ لایه و برنامه اجرایی برای هر مرحله و جزئیات آن‌ها را تشریح نمودیم. همچنین در پایین‌ترین سطح معماری یعنی در لایه عملیاتی گام‌های اساسی برای پیاده‌سازی معماری پیشنهادی ارائه شده است.

معماری‌های مختلفی برای امن‌سازی سیستم‌های سایبری ارائه شده است و هریک با تاکید بر جنبه‌هایی از امنیت روش‌ها و راهبرد و برنامه‌های خود را تشریح کرده‌اند، در این مقاله با ارزیابی معماری‌های مرجع به‌ویژه با الگو گرفتن از مدل NIST که از پرکاربردترین مدل‌های



شکل ۶: اجرای مدل پیشگیرانه پدافند غیرعامل سیستم‌های کامپیوتر

[4] Michael Inden Der Java-Profi: Persistenzlösungen und REST Services dpunkt.verlag pp. 270 2016.

[۵]. مدیری، ناصر، ۱۳۹۹ خودارزیابی و جرم‌شناسی پیشگیرانه

سایبری، موسسه رایان کاویان پویا

[6] Syed Omid Sadjadi "NIST baseline systems for the 2018 speaker recognition evaluation" 2018.

[1] <https://www.nist.gov/cyberframework>.

[2] <https://www.interstell.com/wordpress/security-reference-architecture-the-wheel-does-not-need-reinventing/>

[3] Richardson Maturity Model [online] Available <https://martinfowler.com/articles/richardsonMaturityModel.html>

مراجع

[7] Swaminatha T. The Rise of the NIST Cybersecurity Framework. 11 May 2018. CSO. <https://www.csoonline.com/article/3221139/the-rise-of-the-nist-cybersecurity-framework.html> (21 February 2020, date last accessed).

[8] *Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Alerts*, [online] Available: <https://ics-cert.us-cert.gov/alerts>. (11 Jun 2020, date last accessed).