فصلنامه سیستم‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران
واحد زنجان

معماری امنیت پیشگیرانه سیستم‌های کامپیوتری

DOR: 20.1001.1.27832570.1399.1.1.1.5

یاسمن پولادزاده

دانشکده مهندسی برق و کامپیوتر - دانشگاه آزاد اسلامی واحد تهران شمال - تهران - ایران - yasamanpouladzadeh@yahoo.com

چکیده: مقابله با تهدیدات سایبری به معنی حفاظت از مالکیت مادی و معنوی اطلاعات در تمامی حوزه‌ها و جلوگیری از سوء استفاده است. بنابراین حفاظت از اطلاعات در برابر این تهدیدات، بدون آنکه اختلالی در رشد و توسعه ایجاد شود، یک مسئله 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 تامین 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 , استاندارد ISO 27000 و CERT هستند. مدل پیشگیری یک روش مداخله‌ای برای احتمال به موقع اتفاق افتادن 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 متدلوژی پیشنهادی فازها و فرایند اجرای عملیات مطرح گردیده است.

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

Preventive security architecture of computer systems

Yasaman Pouladzadeh

Faculty of Electrical and Computer Engineering, Islamic Azad University, North Tehran Branch, Iran,
yasamanpouladzadeh@yahoo.com

Abstract: Dealing with cyber threats threats means protecting the material and intellectual property of information in all domains and prevention of abuse. Therefore, protecting information from such threats is an important issue without disturbances in development and development. this issue has now become an important issue, as it is now the most serious challenge for governments to deal with cyber - threats. this area has many approaches to provide cyber - security, one of these approaches is the preventative defense that protects the organization's information.

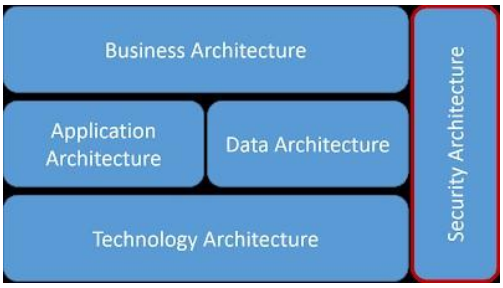
This paper reviews a series of reference architectures[2]and model in cyber - security and provides a new model based on the best practices of each model. The frames and the assessed standards include the NIST framework[1], the ISO 27,000 and CERT[8] standard. Prevention model is an intervention method for the likelihood that the risks have taken place. The proposed model consists of four levels, implementation phases, implementation phases, described in proposed architecture, layers, and programs, and has been proposed in the proposed phases of phases and operations. In the end, based on the need for a preventive model that is never presented And only NIST processes explained.

Keywords: cyber - defense, preventive, security, organization

تاریخ ارسال مقاله: ۱۳۹۹/۰۹/۰۸
تاریخ پذیرش مقاله: ۱۳۹۹/۱۰/۲۳

۱- مقدمه

معماری یک راه‌حل ســـاختاری اســـت که می‌تواند کلیه نیازمندی‌های فنی و عملیاتی مورد انتظار را پو شش دهد. رویکرد ا صلی کار ما SRA ا ست که دا ستن گزینه‌های امنیتی مختلف و نحوه ا ستفاده از آنها در راه‌حل ســـاختاری برای پذیرشـــی موفقیت آمیز و ایمن بســـیار مهم اســـت[۲]. این معماری نمای کلی از مولفه‌های امنیتی برای اســـتقرار، توسعه و عملیات ایمن را نشان می‌دهد. معماری مرجع امنیت سایبری، قابلیت‌های امنیت سایبری و نحوه ادغام آنها با معماری‌ها و قابلیت‌های امنیتی موجود را توصیف می‌کند.



شکل شماره 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 پیاده‌سازیNIST، هدف از این پیاده‌سازی باید مشخص باشد.

۲. **تهیه یک پروفایل دقیق:** گام بعدی، اجرای آزمایشی آن Frameworkبه صورت تخصصی‌تر 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، به‌طوری که می‌توان حالتی خاص را ایجاد نمود.

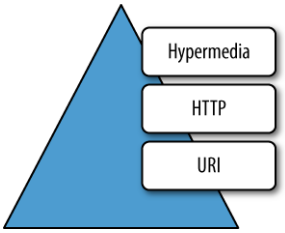
۴. **آنالیز اختلاف بین نتایج و شناسایی اقدامات ضروری:** با مطلع بودن از خطرات امنیت سایبری و تاثیرات تجاری بالقوه برای سازمان، می‌توان فاصله میان نتایج را آنالیز نمود.

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، نهایتا منجر به پیاده‌سازی NIST CSF بصورت مطلوب خواهد شد[۱] [۶].

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 خدماتREST برای شناسایی سطح سررسید آنها، مدل بلوغ ریچاردسون نامیده می‌شود[۳].

شکل شمار ۲: مدل ریچاردسون



شکل۲ طرح لئونارد ریچاردسون است که بر اساس میزان سازگاری با REST، آنها را به چهار دسته تقسیم کرده است[۴].

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

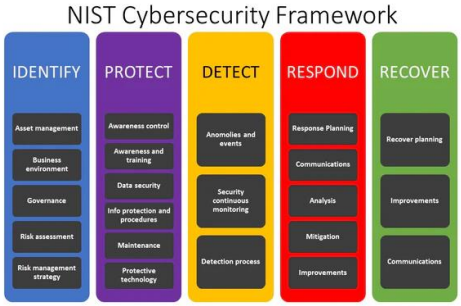
سطح صفر بلوغ از هیچ یک از قابلیت‌هایURI، HTTP و HATEOAS استفاده نمی‌کند. سرویس‌های این سطح یکURI واحد دارند و از یک روش HTTP واحد (معمولاًPOST) استفاده می‌کنند.

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 HATEOASخارج شوند. خدمات سطح دو، میزبان منابع بیشماری با آدرس URI است. سطح دو مورد مناسبی برای استفاده از اصول REST است که طرفدار استفاده از افعال مختلف بر اساس روش‌های درخواست HTTPهستند 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 ریچاردستون 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 همچنین تطبیق و پیاده‌سازی این چارچوب، در عمل کار بسیار دشواری است[۱].



شکل شمار ۳: چارچوب امنیت سایبری در NIST

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

۳- اجرایی نمودن مدل پیشگیرانه

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

جدول شماره 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
	شناسایی ۵ مرحله NIST	شناسایی فعالیت‌های تهدیدات سایبری	اقدامات پیشگیرانه ایمن سازی بانک اطلاعاتی
سطح تاکتیکی	شناسایی تداوم کسب و کار	فعالیت‌های فرآیند و مسئولیت‌ها در صورت هک سامانه	مستندسازی اقدامات پیشگیرانه فعالیت‌های پدافند غیرعامل سایبری
	شناسایی ماموریت‌ها	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 مقرارت
	شناسایی استراتژی تسلط سایبری	مستندسازی فعالیت‌های پدافند غیرعامل سایبری	مستندسازی و کنترل کلاس‌بندی اطلاعات
سطح عملیاتی	شناسایی ریسک‌های سایبری	مستندسازی فعالیت‌های اقدامات پیشگیرانه سایبری	تدوین فرآیند و مسئولیت ها در روش تعریف نیازمندیها
	تدوین برنامه تست نفوذ شبکه و نرم‌افزارها	مستندسازی فعالیت‌های پدافند غیرعامل سایبری	چک لیست اپراتورها

مدل پیشگیرانه پدافند غیرعامل سیستم‌های کامپیوتری دارای۷ 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 فعّال کردن عملکرد شبکه،کتابخانه‌ای از اطلاعات، زنجیره توزیع محتوا و... می‌باشد.

روش‌های مصون‌سازی سایبری شامل دفاع به روش خطی، دفاع بر اساس زون بندی، 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 واکنش گرایانه، پیش‌کنش گرایانه، پیش بینی گرایانه، پیش دستانه می‌باشد.

نوع اقدامات سایبری با توجه به طبقه بندی زیرساخت به ۳ دسته اصلی تقسیم می‌شوند که شامل مصون سازی، استحکام بخشی، ایمن سازی 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 مطرح ترین سیستم‌های تشخیص در حوزه سایبر می‌توان سیستم تشخیص نفوذ (IDS) ، سیستم همبسته ساز رویدادها (IPS)، سیستم تله عسل (Honey pot) را نام برد[۵].

۴- معماری پیشگیرانه

مدل پیشگیرانه دارای ۴ رویکرد مولفه‌ای است که هر رویکرد دارای محیط‌های عملیاتی، از نوع مهم، حساس و حیاتی است و معماری پیشگیرانه شامل مقاوم سازی، استحکام بخشی، جداسازی و مصون‌سازی در چهار سطح شامل سطوح راهبردی تاکتیکی تکنیکی و عملیاتی می‌باشدکه در شکل زیر مشاهده می‌کنید:

شکل شماره ۴: مدل معماری پیشگیرانه

۴-۱ سطح راهبردی

تعیین خطوط کلی رسالت سازمان در بلند مدت

جدول شماره ۲: بررسی سطح راهبردی

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 پاسخ گویی اضطراری کامپیوتر است. که همانند انسان برای آنتی ویروس عمل می‌کنند.
SANS	شرکتSANSیکی از شرکت‌های قدرتمند در حوزه امنیت اطلاعات و یکی از بزرگترین و حرفه‌ای‌ترین تولید کننده آموزش‌های امنیت، تست نفوذ، جرم شناسی است.
FIRST	مجمع جهانی تیم های 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 آســـیب پذیری‌های سیستم عامل‌ها ا ست که به جهت مدیریت ریسک و امنیت دسته بندی 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 فعالیّت‌های علمی، اقتصادی، اجتماعی در جامعه اطّلاعاتی اشاره کرد.
ماهر	مرکز امداد و هماهنگی رایانه ای 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 ماموریت‌های افتا است.

۲-۴ سطح تاکتیکی

فعالیت‌ها برای رسیدن به اهداف میانی سازمان

جدول شماره ۳: بررسی سطح تاکتیکی

تداوم کسب و کار	یک فرایند مدیریت جامع برای شناسایی تهدیدات احتمالی برای یک سازمان و تأثیرات عملیاتی این تهدیدات است.
تداوم ماموریت	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 می‌کنند و به سازمان کمک می‌کنند تا از آسیب بیشتر به عملیات مهم ماموریت جلوگیری کند.
سناریو non CIA	شناسایی اطلاعات و دارایی‌های مربوطه، به علاوه تهدیدات احتمالی، تصمیم گیری در موردچگونگی رفع یا درمان خطرات
استانه تحمل درد سایبری	مقداری که می‌توانیم با تهدیدهای سایبری سازگار باشیم.
NIST	**مشخص نمودن 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 پاسخ گویی اضطراری کامپیوتر است.
رابطه بین NOC,SOC	انعطاف پذیری و به حداکثررساندن دسترسی و کاهش قابل توجه خطر.اطمینان برای شرکت و مشتریان در مورد ایمن نگه داشتن اطلاعات.
تست نفوذ	یک حمله سایبری شبیه سازی 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 دارائی‌ها و سامانه‌ها درقبال حملات، تمرین تصمیم گیری مدیریتی پاسخگو و...
روش دفاع passive	**استتار ، اختفاء ، پوشش ، فریب ، تفرقه و پراکندگی، مقاوم‌سازی و استحکامات اعلام خبر .**
ستون‌های امنیتی	امنیت سایبری خصوصا 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 ساختارIT، اگاهی نیروی انسانی، اهمیت بسیار بالای فاکتور انسانی
Threat Management	مدیریت تهدیدات سایبری (CTM) یک برنامه مدیریت پیشرفته است که امکان شناسایی زود هنگام تهدیدها فراهم می کند.
Thered modling	مدل‌سازی تهدید عملی است برای شناسایی و اولویت بندی تهدیدات احتمالی و تخفیف‌های امنیتی

یاسمن پولادزاده

STRIDE	مراحل مختلف حمله را که از مدل Cyber Kill Chain مشتق شده است، توصیف می‌کند و سپس وظایف اصلی هر مرحله را نشان می‌دهد. در آخر لیستی از TTP متداول را که برای هر کار استفاده می شود، توصیف می‌کند.
DREAD	بخشی از سیستم برای ارزیابی ریسک تهدیدهای امنیتی رایانه است. و شامل آسیب، قابلیت تولید مجدد ، بهره برداری، 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	دسته ای از راه‌حل‌های امنیتی که در برابر بدافزار پیچیده یا حملات مبتنی بر هک با هدف قرار دادن داده های حساس دفاع می کنند.
ATT&CK	لیستی ساختاری از رفتارهای شناخته شده مهاجم است که در تاکتیک‌ها و تکنیک‌ها گردآوری شده و در تعداد انگشت شماری ماتریس و همچنین از طریق STIX / TAXII بیان شده است.
فریب سایبری	مکانیسم‌های کنترل دسترسی سیستم عامل‌های امن پنهان است.

۳-۴ سطح تکنیکی

شامل تکنیک کارهای قبل می‌باشد.

جدول شمار ۴: بررسی سطح تکنیکی

Cyber dominance strategy	سلطه سایبری تهاجمی استراتژیک از سوگیری سواستفاده‌های دشمن با ترکیبی از انفجار اطلاعات و دستکاری سو استفاده می‌کند.
Cyber range	یک محیط مجازی است که شرکت‌ها می‌توانند از آن برای آموزش جنگ سایبری و توسعه نرم افزار 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 نرم افزار سر و کار دارند.
Cwss	مکانیزمی را برای اولویت بندی نقاط ضعف نرم افزار به روشی ثابت، انعطاف پذیر و باز فراهم می‌کند.
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 شده است.
خودارزیابی 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...
KFI	شاخص‌های اصلی کلاهبرداری که رویکرد جدیدی برای راه اندازی و استفاده از شاخص‌های موثر 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 می کنند.
Insider Theread	تهدیدات داخلی، شامل خرابکاری، سرقت، جاسوسی، کلاهبرداری و مزیت‌های رقابتی اغلب از طریق سو استفاده از حقوق دسترسی، و سواستفاده از وسایل فیزیکی انجام می‌شود.
Kali	اصلی‌ترین ابزار مورد نیاز برای یک هکر یا متخصص امنیتی است ومجموعه‌ای عظیم از انواع ابزارهای تست امنیتی در شبکه اینترنت است.
Wire Shark	نرم افزار 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 شده است که توسط افراد تازه وارد در زمینه امنیت برنامه و همچنین تسترهای نفوذ حرفه ای مورد استفاده قرار می‌گیرد.

۴-۴ سطح عملیاتی

فعالیت‌ها گام‌های ویژه جهت رسیدن به اهداف.

جدول شماره ۵: بررسی سطح عملیاتی

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.
ITSM	مدیریت خدمات فناوری اطلاعات به این سادگی است که تیم‌های IT با ارائه خدمات نهایی به مشتریان خدمات را مدیریت می‌کنند.
ISMS	سیستم مدیریت امنیت اطلاعات مجموعه ای از سیاست‌ها و رویه‌ها برای مدیریت سیستماتیک داده‌های حساس سازمان است. هدف ان 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 می‌شود.
اگاهی موقعیتی	به معنی آگاهی محور است و شامل تجزیه و تحلیل، ارزیابی ریسک سازمانی، بررسی سطح شرکت یا روند کارکنان می‌باشد.
مدیریت موضوع SDL	یکی از عناصر اصلی چرخه زندگی توسعه امنیت مایکروسافت است. این یک تکنیک مهندسی است که می‌تواند 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 شبکه‌ها برای شناسایی و جداسازی تهدیدات پیشرفته است.

در ادامه رویکرد اجرایی براساس شکل شماره ۵ معرفی می‌گردد:

شکل شماره ۵: ارائه رویکرد اجرایی

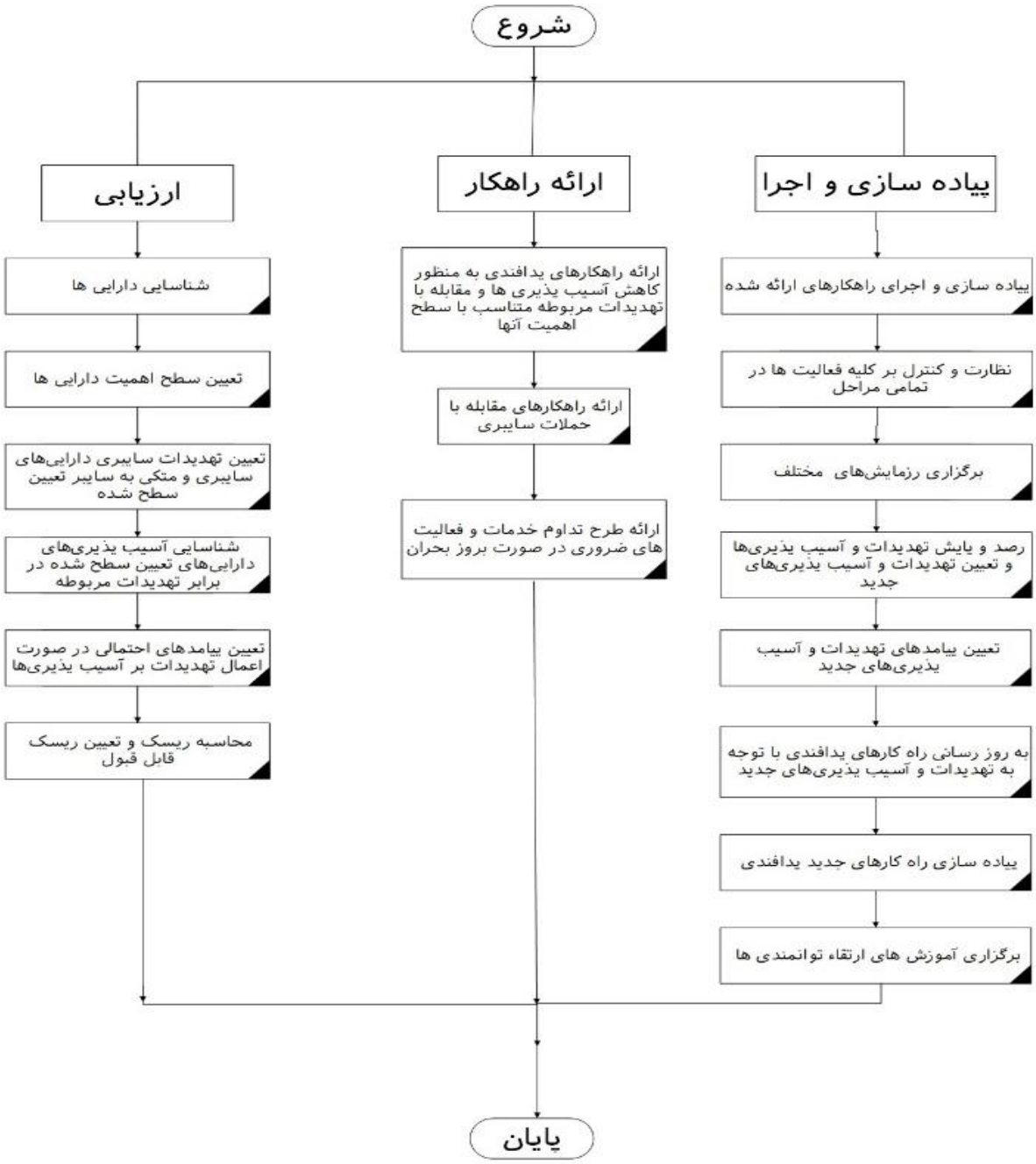
جهت اجرای مدل پیشگیرانه پدافند غیرعامل سیستم‌های کامپیوتری، برنامه اجرای ان شامل ۳ مرحله می‌باشد:

- ارزیابی
- ارائه راهکار
- پیاده سازی و اجرا

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

۵- نتیجه‌گیری

معماری‌های مختلفی برای امن سازی سیستم‌های سایبری ارائه شده است و هر یک با تاکید بر جنبه‌هایی از امنیت روش‌ها و راهبرد و برنامه‌های خود را تشریح کرده‌اند، در این مقاله با ارزیابی معماری های مرجع بویژه با الگو گرفتن از مدل NIST که از پرکاربردترین مدل های مرجع است، و با تحلیل رویکرد و ساختار انها در ارائه یک مدل پیشگیرانه، معماری پیشنهادی این مطالعه که شامل ۴ سطح، ۷ لایه و برنامه اجرایی برای هر مرحله و جزئیات انها را تشریح نمودیم. همچنین در پایین‌ترین سطح معماری یعنی در لایه عملیاتی گام های اساسی برای پیاده سازی معماری پیشنهادی ارائه شده است.



شکل شماره ۶: اجرای مدل پیشگیرانه پدافندغیرعامل سیستم‌های‌کامپیوتر

منابع

[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.

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

[۵]. مدیری، ناصر، ۱۳۹۹ خودارزیابی و جرم شناسی‌پیشگیرانه سایبری، موسسه رایان کاویان پویا

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

[7]SwaminathaT.The Rise of the NIST Cybersecurity Framework. 11 May 2018. CSO. https://www.csoonline.com/article/۳۲۷۱۱۳۹/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. (۱۱Jun ۲۰۲۰, date last accessed).