راه‌اندازی یک واحد پایش امنیت چابک در شرکت‌ها و سازمان‌ها

محمدمهدی قاسمی‌نیا[۱]، محمدحسن میرعارفین[۲]، حسین مرادی[۳]

[۱] کارشناسی ارشد علوم کامپیوتر، دانشگاه یزد، یزد، ایران
ghaseminya@gmail.com
[۲] کارشناسی ارشد مدیریت فناوری اطلاعات، دانشگاه علم و صنعت، تهران، ایران
m_mirarefin@iust.ac.ir
[۳] دانشجوی کارشناسی ارشد مدیریت، دانشگاه تهران، تهران، ایران
ho3in14741@gmail.com

چکیده

ضرورت پیاده‌سازی یک واحد امنیت برای مقابله با تهدیدات محیطی و افزایش ایمنی سازمان، امری غیرقابل انکار است. گسترش روزافزون تهدیدات و پیشرفت‌های نرم و سخت‌افزاری، سازمان‌های بزرگ و کوچک را مجبور به حفاظت بیش از پیش از داده‌ها، سرویس‌ها و دارایی‌هایشان کرده و در این بین، وجود یک تیم منسجم و ساختارمند که بر روی این موضوع متمرکز باشند، امری ضروری است. واحد عملیات امنیت به همین منظور و در جهت مقابله با تهدیدات خارجی و افزایش ایمنی در سازمان تشکیل شده است. مقاله‌ی پیش رو، در آغاز به بررسی و مرور کارها و تحقیقات انجام گرفته در این حوزه می‌پردازد. سپس به شناخت اجزای سازنده‌ی واحد عملیات امنیت در قالب ساختار PPTGC که متشکل از افراد، فرایندها، تکنولوژی، قوانین و رویه‌هاست، پرداخته است. در انتها موارد مستعد تحقیق در این حوزه عنوان شده است.

کلمات کلیدی: واحد عملیات امنیت، امنیت سیستم‌های کامپیوتری، چارچوب پاسخگویی به حادثه، ساختار PPTGC.

۱ مقدمه

براساس آمار یک گزارش که از جمع‌آوری اطلاعات بیش از ۴۷۰۰ شرکت در ۱۸ کشور دنیا در سال ۲۰۲۱ به‌دست آمده، تعداد حملات امنیتی به شرکت‌ها در این سال، با ۳۳ درصد افزایش نسبت به سال ۲۰۲۰، به میانگین ۲۷۰ حمله به ازای هر شرکت رسیده‌است [۱۲]. از جمله دلایلی که می‌توان برای این تعداد حملات گزارش کرد، ضعف سازمان‌ها در داشتن شناختی کامل از مفاهیم و ابزارهای امنیتی سازمان خود، در کنار عدم توانایی در اولویت‌بندی مشکلات و تهدیدات و عدم شناخت کامل و استفاده از ابزارهای موردنیاز برای پاسخگویی به این تهدیدات است. در کنار این موارد، باید به سرعت بالای گسترش فناوری ابزارها، و نیز

پیچیده‌تر شدن حملات و به‌دنبال آن، سخت‌تر شدن شناخت و پاسخگویی به آن‌ها اشاره کرد.

واحد عملیات امنیت، تلاش دارد تا با هرچه واضح‌تر کردن حیطه وظایف، مسئولیت‌ها و ساختار این واحد، به سازمان‌ها در پیاده‌سازی بهتر و موثرتر آن کمک کند. در حالیکه در تصور برخی افراد، وظیفه واحد عملیات امنیت به نظارت بر شبکه داخلی سازمان محدود می‌شود، تعاریف و استانداردهای ارائه‌شده در بخش‌های پیش رو، نشان می‌دهند که این واحد، مرکز تمام عملیات‌های امنیتی سازمان محسوب می‌شود و دامنه گسترده‌ای از وظایف را در بر می‌گیرد.

۲ واحد عملیات امنیت

۱.۲ معرفی

واحد عملیات امنیت، متشکل از تحلیلگران، اپراتورها و متخصصانی است که وظیفه تامین امنیت دستگاه‌های پایانی[1]، زیرساخت تکنولوژی اطلاعات، برنامه‌ها و خدمات سازمان را دارند. اعضای تیم با استفاده از تکنولوژی‌ها و فرایندهای مختلف، در تلاش هستند تا تخطی‌های صورت گرفته از سیاست‌های امنیتی، تلاش‌ها برای اخذ دسترسی‌های غیرمجاز و نیز تهدیدات و حملات صورت گرفته به سیستم‌های سازمان را شناسایی و از آن جلوگیری کرده، یا اثر مخرب آن را کاهش دهند. به‌طور کلی، می‌توان گفت که واحد عملیات امنیت، مسئول حفظ و تعریف چشم‌انداز امنیتی کل سازمان است.

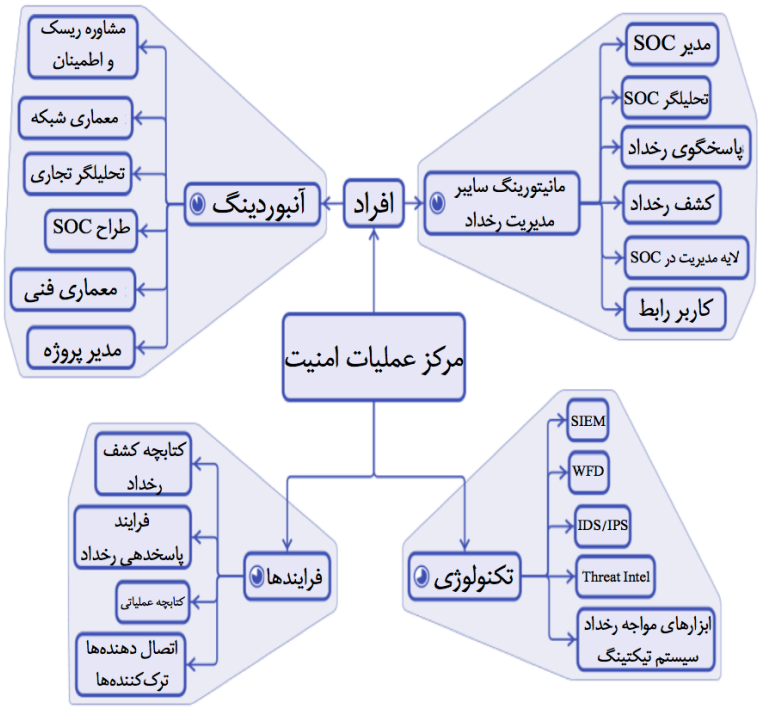
ساختار واحد عملیات امنیت در شکل ۱ قابل مشاهده است [۱۷].

۲.۲ پیشینه تحقیق

از نزدیک به ۱۸ سال پیش که اولین بار واحد عملیات امنیت معرفی شد، تعاریف و وظایف گوناگونی برای آن آورده شده‌است. در یک تعریف، واحد عملیات امنیت، یک واحد متمرکز برای نظارت بر رویدادهای شبکه و پاسخ به حوادث مربوط به رویدادها و حوادث امنیت سایبری است [۸]. مقاله سالانه موسسه SANS که در سال ۲۰۲۲ منتشر شده‌است، اینگونه بیان می‌کند که بیشتر تعاریف از واحد عملیات امنیت، مفاهیمی انتزاعی هستند که هر سازمانی با توجه به امکانات، توانایی‌های افراد و دانش خود آن‌را در جهت حفاظت از خود و پاسخ به تهدیدات محیطی پیاده‌سازی می‌کند که ممکن است همه‌ی از یک ساختار پیروی نکنند [۵]. علی‌رغم وجود اختلاف در بین تعاریف مختلف، شاید اکثر محققین حوزه امنیت بر این تعریف اتفاق نظر داشته باشند که یک مرکز عملیات امنیت، ساختاری پیچیده به منظور مدیریت و بهبود عملکرد امنیتی کل سیستم در یک سازمان است که به کمک فرآیندهای تعریف شده و به طور خاص متمرکز بر تهدید سایبری، نظارت، تحقیقات قانونی، و مدیریت حوادث و گزارش‌دهی فعالیت می‌کند [۱۶].

پس از ذکر تعاریف اولیه، به چارچوب‌های پیشنهادی و اجزای سازنده‌ی واحد عملیات امنیت پرداخته شده‌است. برای نمونه، یک پژوهش با اشاره به وجود سه عامل افراد، فرایندها و تکنولوژی، هماهنگی میان

[1] Endpoint

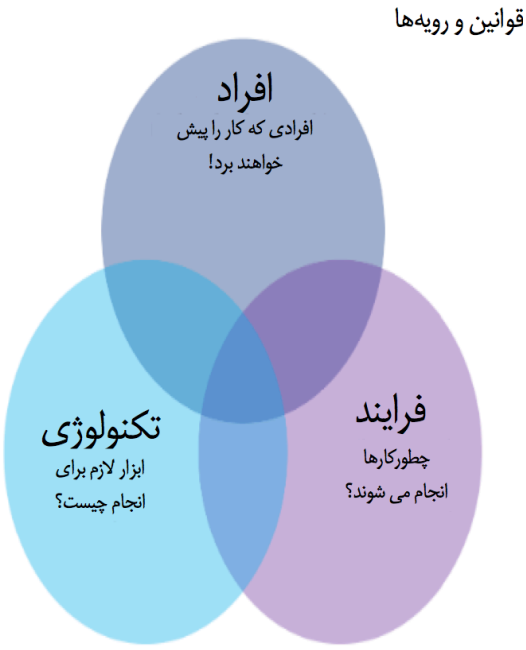


شکل ۱: معماری واحد عملیات امنیت

آن‌ها را عاملی در جهت تشکیل یک تیم واحد عملیات امنیت قوی برمی‌شمارد [۱۰]. پژوهشی دیگر، واحد عملیات امنیت را گروهی از افراد متخصص تعریف می‌کند که از روندها و ابزارها استفاده می‌کنند تا جلوی نفوذ به سیستم را بگیرند [۱۳]. در یکی از جدیدترین تعاریف از ساختار واحد عملیات امنیت، به‌دلیل اهمیت بالای بعد قوانین و رویه‌ها، این بعد از ذیل روندها جدا شده و به یک پایه‌ی اصلی و مستقل در ساختار واحد تبدیل شده‌است [۹]. مشخص است که در همه‌ی منابع مورد بررسی، به سه بعد افراد، روندها و تکنولوژی اشاره شده و در برخی منابع جدیدتر، بعد قوانین و رویه‌ها نیز به‌صورت مستقل بررسی شده‌است.

۳ راه اندازی واحد عملیات امنیت

در این قسمت، به توضیح هریک از ابعاد واحد عملیات امنیت پرداخته می‌شود. این بخش درواقع به افزایش کارایی و بهبود عملکرد واحد عملیات امنیت از طریق تعریف درست روندها، به‌کارگیری ابزار مناسب و استخدام و آموزش افراد شایسته برای جایگاه‌های تعریف شده در واحد می‌پردازد. با مطالعه ادبیات و تحقیقات انجام‌شده در زمینه اجزای سازنده این واحد، مشخص شد که ساختار متشکل از افراد، فرایندها، تکنولوژی، قوانین و رویه‌ها و معروف به PPTGC مطابق شکل ۲ در اکثر موارد پیشنهاد شده‌است [۹].



شکل ۲: اجزای سازنده واحد عملیات امنیت

۱.۳ منابع انسانی–افراد

منظور از افراد، هر جزء انسانی در مجموعه است که از طریق استفاده از ابزارهای فنی و در بستر فرایندها، در جهت تحقق اهداف واحد تلاش می‌کند. در ابتدا، باید افرادی به منظور تشکیل تیم واحد عملیات امنیت انتخاب شوند و سپس، با تشکیل تیم‌ها و تعریف نقش‌ها، مسئولیت به افراد مختلف واگذار شود.

تیم‌های مرکز عملیات امنیت: با حضور حداقل اعضا، اکنون باید برای رسمیت بخشیدن به واحد عملیات امنیت، به تعریف ساختارها و وظایف پرداخت. یکی از چارچوب‌های مورداستفاده در واحدهای عملیات امنیت، بهره‌گیری از سه تیم قرمز، آبی و بنفش است.

تیم قرمز: وظیفه اصلی تیم قرمز، حمله به تیم آبی و تلاش برای از بین بردن سپرهای امنیتی آن است. در واقع اعضای تیم قرمز، هکرهای اخلاقی[۲] هستند که نه با هدف سوءاستفاده، بلکه با هدف شناسایی نقاط ضعف سیستم به آن حمله می‌کنند [۴] [۹].

مهم‌ترین ابزارهایی که تیم قرمز از آن‌ها استفاده می‌کند، عبارتند از: تست نفوذ[۳] که با هدف شناسایی نقاط ضعف اپلیکیشن، شبکه و ابزارهای مورداستفاده یک سیستم اجرا می‌شود [۴]. نکته مهم در این خصوص، این

[2] Ethical hackers
[3] Penetration testing

است که اجراکنندگان تست نفوذ، بیشتر از آنکه به‌دنبال یافتن آسیب‌پذیری‌های کاملا جدید[۴] باشند، در صدد استفاده از آسیب‌هایی هستند که پیش از این شناخته شده، اما هنوز توسط توسعه دهنده سیستم برطرف نشده‌اند.

ابزارهای جعل هویت مانند فیشینگ[۵] و مهندسی اجتماعی[۶]. مهندسی اجتماعی، فرایند نفوذ به یک سیستم، با استفاده از نفوذ به افراد آن سیستم است که در اغلب مواقع، قدمِ پیش از نفوذ فنی می‌باشد [۱۵].

ابزارهای پیمایش درگاه‌ها و شبکه[۷] که در تلاش برای شناسایی درگاه‌های باز[۸] و ارتباطات ورودی و خروجی شبکه سیستم است. در عین حال که می‌توان از ابزارهای آماده نظیر زن‌مپ[۹] و وایرشارک[۱۰] برای این موارد استفاده کرد، برای دسترسی به اطلاعات دقیق‌تر و جزئیات اضافه، می‌توان به کمک کتابخانه‌های قدرتمند زبان‌هایی مثل پایتون و C، ابزارهایی را از ابتدا توسعه داد تا امکان کنترل بیشتر ر روی سیستم نیز مهیا باشد.

یکی از مهم‌ترین اقدامات پس از حملات آزمایشی، نگارش دقیق گزارش حملات است. این گزارش‌ها، شامل ۲ بخش است که در بخش اول، مواردی نظیر ابزارهای فنی مورداستفاده، اهداف مورد حمله و تلاش‌های موفق و ناموفق ذکر می‌شود. در بخش دوم نیز تیم قرمز به ارائه پیشنهادات و راهکارهای افزایش امنیت سیستم اشاره می‌کند. این گزارش‌ها در ادامه، مورد استفاده‌ی تیم آبی قرار خواهند گرفت.

تیم آبی: در نقطه مقابل تیم قرمز، تیم آبی قرار دارد که وظیفه اعضای آن، حفظ امنیت سیستم در مقابل تهدیدات و حملات، ارزیابی فنی ابزارهای مورد استفاده و کشف، شناسایی و از بین بردن آسیب پذیری‌های سیستم است [۳].

مهم‌ترین وظایف تیم آبی عبارتند از:

- نظارت بر عملکرد سیستم
- تشخیص و از بین بردن تهدیدات و حملات امنیتی
- جمع‌آوری داده‌های مربوط به ترافیک داخلی و خارجی شبکه و تحلیل آن‌ها
- پیاده‌سازی و مدیریت ابزارهای کنترل دسترسی کاربران
- به‌روزرسانی ابزارها و نرم‌افزارهای مورداستفاده
- اجرای مهندسی معکوس بر روی حملات صورت گرفته به سامانه‌های مجموعه

[4] Zero days
[5] Phishing
[6] Social Engineering
[7] Port and network scanner
[8] open ports
[9] Zenmap
[10] Wireshark

- طراحی و توسعه سیاست‌های پاسخ فوری جهت اطمینان از بازگشت سریع سیستم به حالت عادی پس از بروز حمله

یکی دیگر از وظایف مهم تیم آبی، به‌روز نگه‌داشتن دانش افراد و سرمایه انسانی مجموعه در جهت مقابله با تهدیدات است. در جایی‌که تیم قرمز، و نیز تهدیدات دنیای واقعی از ابزارهای مهندسی اجتماعی برای نفوذ به افراد استفاده می‌کنند، مقابله با آن‌ها وظیفه تیم آبی بوده تا با ارتقای دانش اعضا در خصوص جدیدترین تهدیدات انسانی در حوزه‌های مهندسی اجتماعی و جعل هویت، و نیز تعیین سیاست‌هایی در حوزه‌هایی مثل رمزهای عبور [۱۱]، از خطرات احتمالی جلوگیری کند.

همانند تیم قرمز، تیم آبی نیز باید به طور منظم از فعالیت‌های خود گزارش تهیه کرده و در آن، ضمن جمع‌آوری مدارک و لاگ‌های به دست آمده از حادثه، تجربیات تیم از این اتفاق و نیز اقدامات پیش‌رو را ذکر کند.

تیم بنفش: عنوان تیم برای تیم بنفش، شاید به طور کامل درست نباشد؛ از آن جهت که بیشتر از آنکه این تیم، یک تیم مستقل با اعضایی جدا باشد، ترکیبی از اعضای تیم‌های قرمز و آبی است که وظیفه اصلی آن، ایجاد و تسهیل ارتباط بین اعضای این دو تیم در جهت اشتراک‌گذاری یافته‌هایشان است[۳].

علی رغم وظیفه مشترک هر دو تیم قرمز و آبی در بهبود امنیت و کارایی سیستم، گاهی اوقات آن‌ها از به اشتراک گذاری رازهای خود امتناع می‌کنند؛ به این معنی که تیم قرمز، اطلاعات دقیقی از نحوه آسیب به سیستم را در اختیار تیم قرمز نمی‌گذارد، و تیم آبی نیز از نحوه کشف و یافتن جزئیات حملات تیم قرمز و مقابله با آن‌ها صحبت چندانی نمی‌کند. دلیل اصلی تشکیل تیم بنفش، که در واقع ترکیبی از اعضای این دو تیم است، همین تسهیل ارتباط است تا دانش به‌دست آمده از فعالیت‌های دو تیم، راحت‌تر به دیگری منتقل شود تا توسعه و پایدارسازی سیستم دچار مشکل نشود.

نقش‌ها و وظایف اعضای واحد عملیات امنیت: یک واحد عملیات امنیت، دارای ۴ دسته جایگاه اصلی به شرح ذیل است[۶][۲][۹]:

۱. نقش‌های مدیریتی

- هماهنگ‌کننده تیم پاسخگویی به حادثه [۱۲]
- مدیر واحد عملیات امنیت [۱۳]
- مدیر ارشد امنیت اطلاعات [۱۴]

۲. نقش‌های پاسخگویی به حادثه

[11] Password policies
[12] Incident response coordinator
[13] SOC manager
[14] Chief information security officer(CISO)

- پاسخگوی اولیه حادثه[۱۵]
- محقق امنیت[۱۶]
- تحلیلگر ارشد امنیت[۱۷]

۳. نقش های مشاوره‌ای

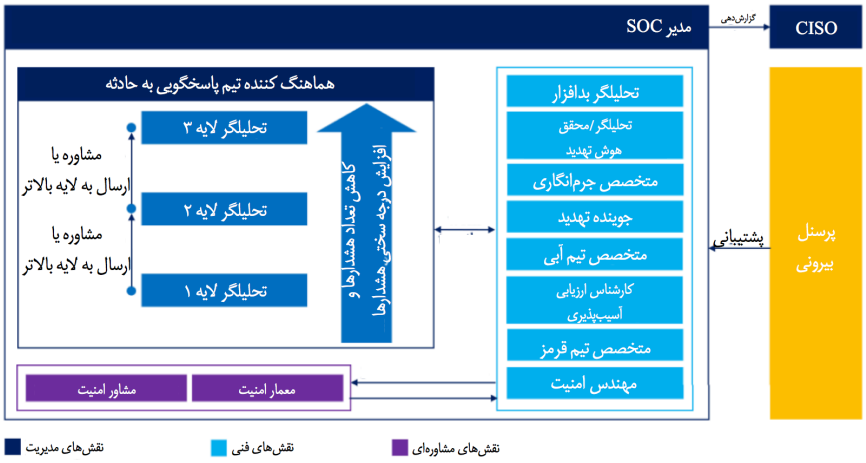
- معمار امنیت[۱۸]
- مشاور امنیت[۱۹]

۴. نقش‌های تکمیلی

- تحلیلگر بدافزار[۲۰]
- جوینده تهدید[۲۱]
- تحلیلگر/محقق هوش تهدید[۲۲]
- متخصص جرم‌انگاری[۲۳]
- متخصص تیم قرمز و تیم آبی
- کارشناس ارزیابی آسیب پذیری[۲۴]
- مهندس امنیت[۲۵]

وجود این نقش‌های مختلف در کنار یکدیگر، نیازمند ساختاری منسجم است تا نتیجه مطلوب که تامین امنیت سازمان است، حاصل شود. شکل ۳، مدلی پیشنهادی از نحوه ارتباط این نقش‌ها با یکدیگر است. مطابق این ساختار، افراد خارج از واحد عملیات امنیت، برای حصول نتیجه بهتر، با این واحد همکاری می‌کنند [۹].

[15] Incident responder
[16] Security investigator
[17] Advanced security analyst
[18] Security architect
[19] Security Consultant
[20] Malware analyst
[21] Threat hunter
[22] Threat intelligence analyst/researcher
[23] Forensics specialist
[24] vulnerability assessment expert
[25] Security engineer

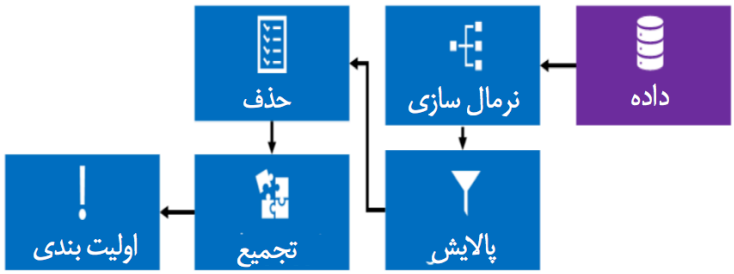


شکل ۳: نحوه ارتباط نقش‌های مختلف در واحد عملیات امنیت

۲.۳ ابزارها

اعضای تیم عملیات امنیت به منظور پیاده‌سازی فرایندها، به ابزارهایی نیاز دارند تا در بخش‌های مختلف از آن‌ها استفاده کنند. ۳ بخش اصلی ابزارهای این واحد به شرح زیر هستند:

۱. **جمع‌آوری اطلاعات**[۲۶]: اولین گام پیش از هرگونه اقدامی در سیستم، داشتن اطلاعات کافی از بخش‌های مختلف آن است. جمع‌آوری داده مراحل مختلفی را طی می‌کند تا به شکلی منظم و قابل فهم درآید. مراحل جمع‌آوری داده، مطابق شکل ۴ نمایش داده شده‌است [۹].



شکل ۴: فرایند جمع‌آوری داده‌ها

[26] Data collection

(آ) نرمال‌سازی: در بررسی تحقیقات، اغلب از نرمال سازی با عنوان پیش‌پردازش داده‌ها یاد شده‌است. این مورد به آن معنی است که داده‌های جمع‌آوری شده باید تحت یک قالب یکسان قرار گرفته و موارد ناهمگون احتمالی، یک شکل و استاندارد ثابت به خود بگیرند. مهم‌ترین نکته در هماهنگی داده‌ها، پیروی کردن همه‌ی آن‌ها از یک قالب متنی و زمانی استاندارد و یکسان است تا امکان استفاده ا آن‌ها در قالب مقایسه فراهم شود [۱].

(ب) پالایش و حذف: از آنجایی‌که دستگاه‌های موجود در سیستم، حجم بزرگی از داده‌ها را تولید می‌کنند، در این مرحله باید موارد کم‌اهمیت‌تر از دور خارج شوند تا داده‌های اصلی قابل استفاده باشند [۷].

(ج) تجمیع و اولویت‌بندی: موارد مختلفی از داده‌های تولیدشده که مشابه هستند، تجمیع می‌شوند و سپس موارد مهم‌تر که باید سریع‌تر مورد توجه قرار بگیرند، مشخص می‌شوند [۷].

پس از شناخت مراحل تبدیل داده‌های خام جمع‌آوری شده به داده‌های قابل استفاده، باید انواع سیستم‌های اطلاعاتی را شناخت. این سیستم‌ها دسته‌بندی‌های مختلفی دارند [۹] مانند: سیستم‌های اطلاعاتی توزیع‌شده[۲۷] / مرکزی[۲۸]، سیستم‌های اطلاعاتی جزئی[۲۹] / کامل[۳۰] و سیستم‌های اطلاعاتی بلادرنگ[۳۱] / تجمیعی[۳۲]

بخش‌ها و ابزارهای مختلفی در سیستم می‌توانند به جمع‌آوری داده بپردازند که به برخی از آن‌ها اشاره خواهد شد:

(آ) نرم‌افزارهای امنیتی نظیر سیستم‌های تشخیص/جلوگیری از ورود و دیوارآتش

(ب) ابزارهای شبکه مانند سرورها و روترها

(ج) بسترهای مجازی‌سازی نظیر مجازی‌سازها[۳۳]

(د) ابزارهای عملیاتی نظیر حسگرها[۳۴] و محرک‌ها[۳۵]

(ه) سایر نرم‌افزارها مانند پایگاه‌های داده و سیستم‌عامل‌ها

(و) ابزارهای فیزیکی مثل دوربین‌های نظارتی و سیستم‌های ورود و خروج[۳۶]

[27] Distributed
[28] Centralized
[29] Partial
[30] Full
[31] Real-time
[32] Historical
[33] Hypervisor
[34] Sensor
[35] Actuator
[36] Access control systems

(ز) افراد

بسته به میزان و نوع نیاز سازمان، کمیت و کیفیت استفاده از ابزارهای مختلف به منظور جمع‌آوری داده متفاوت است. در عین حال که جمع‌آوری داده‌های کم، می‌تواند منجر به ناشناس ماندن تهدیدات شود و امنیت سیستم را مختل کند، جمع‌آوری داده‌های زیاد نیز منجر به کاهش عملکرد سیستم می‌شود.

۲. **آنالیز و تشخیص**[۳۷]: با وجود گسترش ابزارهای تشخیص خودکار حملات، برخی از حملات پیچیده را نمی‌توان به این صورت شناسایی کرد که نیازمند مداخله انسانی به این منظور است. در این بین، از ۳ روش اصلی به شرح زیر، برای شناسایی حملات و تهدیدات متوجه سیستم، استفاده می‌شود:

(آ) شناسایی مبتنی بر ناهنجاری[۳۸]
این روش، رفتار عادی سیستم را به عنوان یک مبنا در نظر گرفته و انحراف از عملکردهای پیش‌آمده را از طریق مقایسه شناسایی می‌کند.

(ب) شناسایی مبتنی بر دانش[۳۹]
این روش بیشتر برای شناسایی حملات تکراری و مشابه استفاده می‌شود و در آن، از دانش تجمیع شده که از حملات قبلی به‌دست آمده‌اند، به عنوان تجربه استفاده می‌شود.

(ج) شناسایی مبتنی بر معیار[۴۰]
در روش شناسایی مبتنی بر معیار، با استفاده از نمایه‌ها[۴۱] و قراردادهای از پیش تعیین‌شده[۴۲]، حوادث تشخیص داده می‌شوند.

۳. **ارائه**[۴۳]: آخرین دسته از ابزارها، جهت نمایش رفتار سیستم به‌کار می‌روند. به منظور مدیریت بهتر بخش‌های مختلف سیستم، نیاز است تا داده‌های جمع‌آوری شده و یا تهدیدات شناسایی شده در ۲ بخش گذشته، به شکلی نمایش داده شوند تا به جز اعضای خبره‌ی واحد عملیات امنیت، برای سایر اعضای کم‌تجربه‌تر این واحد و یا اعضای سایر واحدها قابل فهم باشند. به این منظور در اغلب مواقع از داشبورهای گرافیکی استفاده می‌شود.

[37] Analysis & detection
[38] Anomaly-based detection
[39] Knowledge-based detection
[40] Specification-based detection
[41] Profile
[42] Protocols
[43] Presentation

۳.۳ رویه و دستورالعمل‌ها

است که صرفا مشخص می‌کند چه کاری باید انجام شود و نحوه انجام آن را مشخص نمی‌کند. چارچوب‌ها اغلب منعطف و ماژولار اند؛ به این معنی که قابلیت کم و زیاد کردن بخش‌های مختلف بسته به نیاز مجموعه وجود دارد و یک ساختار خشک و غیرقابل تغییر نیستند.

این چارچوب که توسط موسسه ملی استاندارد و تکنولوژی آمریکا توسعه داده شده‌است، دارای ۴ مرحله اصلی به شرح زیر است [۱۴] :

۱. آماده‌سازی[۴۴]

این مرحله ناظر به آماده‌سازی ابزارها و تجهیزات موردنیاز برای مقابله با تهدیدات است و به طور کلی شامل مواردی نظیر مهیاکردن ابزارهای فنی، آموزش کارکنان و سیاست‌های پاسخگویی به تهدیدات و روندهای مقابله با آنها، و نیز آماده‌سازی سیستم تشخیص تهدیدات است. در این بخش، ابتدا باید به اولویت‌بندی حملات پرداخت.

به‌این منظور، اعضای تیم باید لیستی از حملات رایج تهیه کرده، و سپس به صورت خاص درجه اهمیت هریک را گزارش کنند. شایع‌ترین حملات به سیستم‌های فناوری و اطلاعاتی عبارتند از [۱۱]:

(آ) بررسی درگاه‌های باز سیستم[۴۵]: در اغلب مواقع، اولویت پایینی داشته و اگر نشانه‌های دیگری مبنی بر وجود حمله گزارش نشوند، باید نادیده گرفته شوند.

(ب) آلودگی از طریق بدافزار[۴۶]: در این مواقع باید هرگونه ردی از بدافزار به‌سرعت از سیستم پاک شده و سپس با بررسی دقیق، اطمینان حاصل شود که ردی از بدافزار باقی نمانده‌است. این حملات معمولا اولویت متوسط دارند.

(ج) حملات انکار خدمت[۴۷] : بسته به طول مدت ادامه‌دار بودن این حملات، می‌توانند اولویت پایین یا بالایی داشته‌باشند. پاسخ مناسب در مقابل این دست حملات، سدکردن راه درخواست‌های مخرب به‌نحوی است که عملکرد کلی سیستم دچار خدشه نشود. معمولا می‌توان از طریق مدیریت سرویس‌ها و دستگاه‌های لبه‌ی شرکت (که مستقیما با اینترنت در ارتباط بوده و در معرض حمله هستند) و یا حتی ارتباط با ارائه‌دهنده خدمت اینترنت[۴۸] مبنی بر مسدودسازی برخی درخواست‌ها به مقصد سامانه‌های سازمان، به این مهم دست یافت.

(د) دسترسی غیرمجاز[۴۹] : این دسته از دسترسی‌ها، چه توسط کاربران داخلی سازمان و چه توسط مهاجمین بیرونی، باید به‌سرعت قطع شده و اقدامات بعدی لازم نظیر بازنگری قوانین و

[44] Preparation
[45] Port Scanning
[46] Malware Infection
[47] Denial of Service Attacks
[48] Internet Service Provider
[49] Unauthorized Access

رویه‌های دسترسی و تغییر گذرواژه‌های ضعیف انجام گیرند. این دسته از حملات که مهاجم به درون سیستم نفوذ کرده، اولویت بالایی دارند و باید در اولین فرصت بررسی شوند.

(ه) حملات سطح اینترنت: این دسته از حملات شامل مواردی نظیر XSS، SQL Injection و CSRF می‌شوند که از اولویت بالایی برخوردار بوده و معمولا با بررسی گزارش رخداد پایگاه‌داده [۵۰]، قوانین و رویه‌های حاکم بر سرویس‌ها و فایل‌های تنظیمات برنامه‌ها [۵۱]، قابل ردیابی به نقطه وقوع حمله و سپس از بین بردن آن است.

پس از دفع خطر حمله و برقراری آرامش نسبی، باید اقدام به تهیه راهنمای پاسخ به حملات کرد. بدیهی است که ثبت روند پاسخ به حملات، مخصوصا حملاتی که برای دفعات اول صورت گرفته و هنوز شیوه دقیق پاسخ به آن پیدا نشده‌است، امری ضروری است؛ چراکه با تکرار این حملات در سازمان، اگر چارچوبی برای ثبت و ضبط دقیق این موارد موجود نباشد، ممکن است نیاز باشد هر بار روند از ابتدا و همراه با آزمون و خطا طی شود که اینگونه، علاوه بر افزایش آسیب‌پذیری سیستم، سرعت و دقت در پاسخگویی به حملات نیز کاهش می‌یابد. افزون براین، با خروج اعضای قدیمی و جایگزینی اعضای جدید به‌جای آنان، نیاز به وجود چنین اسنادی بیش‌از پیش احساس می‌شود تا اعضای جدید، به جای آغاز روند تحقیق و توسعه از صفر، ادامه کارهای گذشته را پیش ببرند.

۲. تشخیص و بررسی [۵۲]

پس از آماده‌سازی سیستم تشخیص تهدیدات در مرحله ۱، هنگامی که نشانه‌هایی از ورود به سیستم مشاهده یا گزارش شود، وارد مرحله ۲ می‌شویم. این مرحله، خود شامل ۲ بخش بوده و در بخش اول که تشخیص خطر است، علامت‌هایی توسط نشانگرهای [۵۳] سیستم‌های نظارتی مشاهده شده و سپس روند گزارش‌دهی و طی مراحل بعدی آغاز می‌شود. در این مرحله می‌توان از سیستم‌های نظارتی در حوزه‌های مختلفی نظیر دیوار آتش [۵۴]، سیستم‌های تشخیص/ پیشگیری نفوذ [۵۵] و سیستم‌های آنالیز پهنای باند شبکه [۵۶] استفاده کرد.

در بخش دوم این مرحله، نوبت به آنالیز داده‌های دریافتی از نشانگرهای بخش قبلی می‌رسد. در اینجا، یک متخصص آنالیز حادثه باید تایید کند که آیا واقعا حادثه اتفاق افتاده است یا خیر. دلیل این امر، وجود خطاهای مثبت کاذب [۵۷] است که در آن، طبق داده‌های حاصل از نشانگرها یک نفوذ وجود دارد، اما در واقع خطری سیستم را تهدید نمی‌کند. این وظیفه یکی از مهم‌ترین و سخت‌ترین وظایف

[50] DataBase Logs
[51] Application Configuration Files
[52] Detect and analysis
[53] Indicators
[54] Firewall
[55] Intrusion detection/prevention systems
[56] Network traffic analysis systems
[57] False positive

در روند پاسخگویی به حادثه است و باید فرد یا افرادی باتجربه و بامهارت مسئولیت آن را به عهده بگیرند.

۳. نگهداری، از بین بردن و بازیابی[۵۸]

این مرحله دارای ۳ بخش است که در بخش اول، وظیفه نگهداری به معنی جلوگیری از بدتر شدن شرایط است و در ادامه باید به مرور کنترل سیستم را مجددا به دست گرفت.

بخش دوم، از بین بردن خطر است و شامل حذف بدافزار مخرب و یا قطع دسترسی و حذف کاربران مشکوک است.

در مرحله آخر، بازیابی سیستم به حالت عادی در دستور کار است و این کار، به‌کمک بازگردانی پشتیبان‌ها[۵۹]، نصب مجدد برخی نرم‌افزارها و تغییر گذرواژه‌های نامطمئن صورت می‌گیرد.

۴. فعالیت‌های پساحادثه[۶۰]

تمرکز مرحله آخر، بر روی درس‌های آموخته شده از حادثه و با ۲ محور است: اول آنکه توانایی پاسخگویی به حادثه در مجموعه افزایش یابد و به طور کلی آسیب‌پذیری در مقابل تهدیدات کاهش پیدا کند. دوم اینکه از تکرار اتفاقات مشابه در آینده جلوگیری شود. در این مرحله، به منظور کسب تجربه بهتر از حادثه رخ داده، تیم باید به چند سؤال پاسخ دهد، از جمله: دقیقا چه اتفاقی افتاد؟ چه چیزی خوب پیش رفت؟ چه چیزی خوب پیش نرفت؟ کدام افراد کارشان را به خوبی انجام دادند؟ کار چه کسانی می‌توانست بهتر انجام شود؟ کدام روندها به درستی اجرا شد؟ کدام روندها می‌توانستند بهتر انجام شوند؟ چگونه می‌توانستیم چلوی این اتفاق را بگیریم؟ با پاسخگویی دقیق به سؤالات بالا و سؤالاتی از این دست، می‌توان گزارشی دقیق از حادثه تهیه کرد تا ضمن ارتقای دانش مجموعه در مواجه با حوادث مشابه، پاسخگویی کلی نیز بهبود یابد.

۴ سخن پایانی

در این نوشته یک روشی برای ایجاد یک تیم واحد عملیات امنیت به همراه گام‌های راه‌اندازی و اهداف نهایی ارائه گردید، همچنین تفکیک اجزا و مشخص کردن راهبرد و راهبری کلی اجزا، تیمها و نقش‌ها در کنار هدف اصلی اجزا و چگونگی ارتباط آنها با هم به شکل کامل در اختیار خواننده قرار گرفت.

به عنوان موضوعات مستعد تحقیق بیشتر می توان در مورد بررسی ایرادات ممکن در استانداردهای بین‌المللی از قبیل ایزو در حوزه امنیت و تقابل آن با رویکردهای فضای سایبر جمهوری اسلامی ایران سخن گفت و همچنین چگونگی افزایش امنیت فضای سایبر جمهوری اسلامی ایران با الگو قراردادن این استانداردهای موجود، و باز تولید استاندارد بومی نیز می‌تواند زمینه های تحقیقاتی بعدی باشد.

[58] containment, eradication and recovery
[59] backups
[60] Post incident activity

سپاس‌گزاری

خدا را شاکریم که به ما کمک داد تا بتوانیم هر چند کوچک قدمی در حوزه فضای سایبر برداریم. از سازمان صدرا بابت پشتیبانی کامل در قالب یک پروژه پژوهشی و کمکهای بی دریغشان در تولید این مقاله نهایت سپاسگزاری را داریم.

مراجع

[1] S. Rezayi A. Madani and H. Gharaee. Log management comprehensive architecture in security operation center (soc). *Int. Conf. Comput. Aspects Social Netw. (CASoN)*, page 284–289, Oct 2011.

[2] O. Cassetto. Security operations center roles and responsibilities. *Exabeam, Foster City, CA, USA, Tech. Rep*, 2019.

[3] Svitlana Chaplinska. A purple team approach to attack automation in the cloud native environ-ment. *Aalto University*, 2022.

[4] Matthias Caretta Crichlow. A study on blue team's opsec failures. 2020.

[5] C. Crowley and B. Filkins. Sans 2022 security operations center survey. In *SANS Inst*, volume Swansea, U.K., 2022.

[6] Carson Zimmerman Kathryn Knerler, Ingid Parker. 11 strategies of a world-class cyber-security operations center. *MITRE Corp Bedford, MA, USA, Tech. Rep*, 2022.

[7] K. Kent and M. Souppaya. Guide to computer security log management: Recommendations of the national institute of standards and technology. *Nat. Inst. Standards Technol., Gaithersburg, MD, USA Tech. Rep. 800-92*, 2006.

[8] J. Mtsweni M. Mutemwa and L. Zimba. Integrating a security operations centre with an organization's existing procedures, policies and information technology systems. In *Intell. Innov. Comput. Appl. (ICONIC)*, page 1–6, Dec 2018.

[9] I. Fichtinger M. Vielberth, F. Böhm and G. Pernul. Security operations center: A systematic study and open challenges. *IEEE Access*, 8:227756–227779, 2020.

[10] M. Majid and K. Ariffi. Success factors for cyber security operation center (soc) establishment. In *1st Int. Conf. Informat., Eng., Sci.Technol.*, number Bandung, IN, USA, page 1–11, May 2019.

[11] J. Anuradha Mohan V. Pawar. Network security and types of attacks in network, procedia computer science. 48:503–506, 2015.

[12] NAdara. How aligning security and the business creates cyber resilience. *Accenture*, New York, NY, USA, 2021.

[13] C. Onwubiko. Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. In *International Conference on Cyber Situational Awareness*, volume Data Analytics and Assessment (CyberSA), 2015.

[14] T. Grance P. Cichonski, T. Millar and K. Scarfone. Computer security incident handling guide: Special publication 800-61 revision 2. *Nat. Inst. Standards Technol*, 2012.

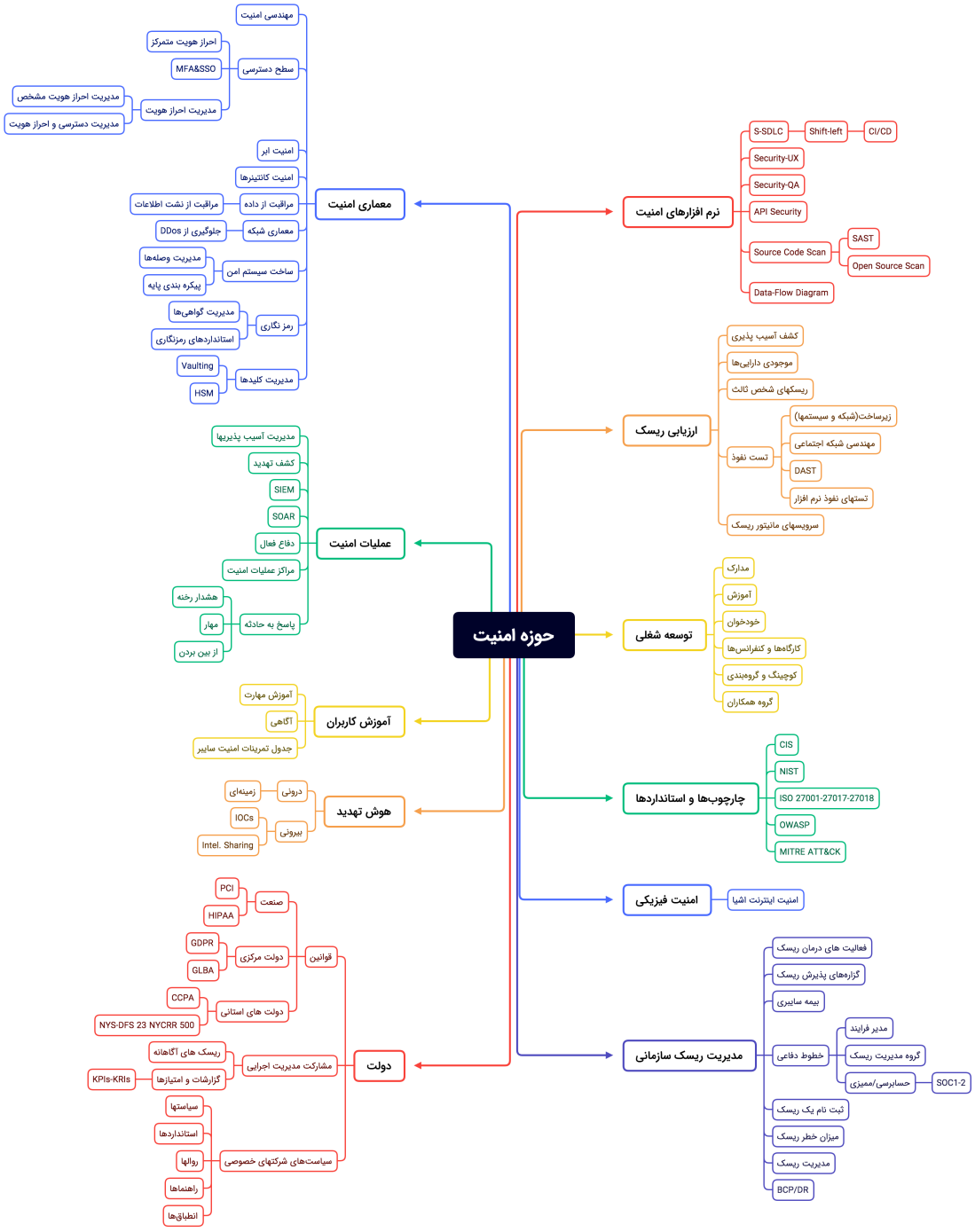
[15] Kaabouch N. Social Engineering Attacks Salahdine F. A survey. future internet. 2019.

[16] Keith & Paans Ronald Schinagl, Stef & Schoon. A framework for designing a security operations centre (soc). *10.1109/HICSS.2015.270*, pages 2253–2262, 2015.

[17] R. Vaarandi and S. Mäses. How to build a soc on a budget. *IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece*, pages 171–177, 2022.

پیوست

درخت دانش حوزه امنیت سایبر



شکل ۵: درخت دانش حوزه امنیت سایبر