پنجمین کنفرانس ملی فناوری های نوین در مهندسی برق و کامپیوتر
۳۰ شهریور ماه ۱۴۰۱ - اصفهان
ISC
پایگاه استنادی علوم جهان اسلام
۰۱۲۲۰-۹۰۱۳۵

آگاهی وضعیتی در دفاع سایبری فعال، راهبردی به منظور مقابله با حملات پیشرفته امروزی

حامد رادی نیا، کارشناسی ارشد مهندسی کامپیوتر گرایش رایانش امن، h.radinia@gmail.com[۱]
علی جبار رشیدی، دانشیار و عضو هیئت علمی، rashidi@mut.ac.ir[۲]

چکیده

امروزه حملات پیشرفته‌ی سایبری، با ضربه زدن به زیرساخت‌های حیاتی خطرهای جدی را برای اقتصاد و امنیت ملی کشورها پدید آورده‌اند. متاسفانه غالبا مهاجمین و بدافزارهای رایانه‌ای یک قدم از سیستم‌های امنیتی جلوتر می‌باشند. از این رو باید به جای انتظار برای مواجهه با تهدیدات و هجمه‌های احتمالی، یعنی همان روش‌های پیشین دفاع سایبری، به دنبال راه‌حلی قوی‌تر و هوشمندانه‌تر برای از میان بردن آن خطر احتمالی باشیم. اینجاست که نظریه "دفاع سایبری فعال" مطرح می‌شود که بخش اساسی آن آگاهی وضعیتی سایبری می‌باشد. طی چند سال اخیر دفاع سایبری فعال و آگاهی وضعیتی به عنوان یک راهبرد جدید دفاعی در حوزه سایبر، بین متخصصان و دانشمندان جهانی مورد بحث و بررسی قرار گرفته است و کشورهای بزرگ دنیا راهبردهای دفاعی خود را بر مبنای آن تبیین می‌کنند. هر کشور بر اساس زیرساخت‌های داخلی و ساختار خود، تعریف و رویکردی متفاوت از دفاع سایبری فعال دارد. در این بین، کشور ایران به عنوان یکی از قدرت‌های سایبری دنیا باید به این سمت حرکت نموده و راهبردهای دفاعی خود را متناسب با تهدیدات به روز نماید.

در این مقاله ضمن ارائه یک تعریف جدید از دفاع سایبری فعال و جمع‌آوری تکنیک‌های منحصر به فرد آن، بر اثربخشی و بازدارندگی این نوع دفاع تاکید می‌گردد. در ادامه با بررسی برخی از ابعاد دفاع سایبری فعال و بخش اساسی آن یعنی آگاهی وضعیتی سایبری، لزوم ارائه یک مدل گسترده آگاهی وضعیتی بر مبنای راهبردها و تکنیک‌های این نوع دفاع نشان داده می‌شود.

دفاع سایبری، دفاع فعال، دفاع سایبری فعال، آگاهی وضعیتی، آگاهی وضعیتی سایبری، بازدارندگی

۱- مقدمه

امروزه حملات سایبری دارای پیچیده‌گی‌های زیادی هستند و نفوذگران باهوش‌تر از گذشته با شناسایی دقیق شبکه مورد نظر و طی کردن یکسری از دستورالعمل‌های از پیش تعیین شده حملات خود را آغاز می‌نمایند[۶]. دولت‌ها در سراسر جهان، به منظور حفاظت از زیرساخت‌های اطلاعاتی حساس، راهبردها و قابلیت‌های امنیتی یا برنامه‌های پاسخ به حادثه ملی را درون چشم انداز تهدید جدید در عصر سایبری قرار می‌دهند.

مَشی کلی و متداولی که نفوذگرانی حرفه‌ای برای حمله به شبکه استفاده می‌کنند به خوبی قابل فهم می‌باشد[۶]. جمع‌آوری اطلاعات، شناسایی هدف، برنامه ریزی اولیه و توسعه آن، شناسایی شبکه، دنبال نمودن برنامه و آماده‌سازی، حمله و ارزیابی

[۱] دانشگاه صنعتی مالک اشتر تهران
[۲] دانشگاه صنعتی مالک اشتر تهران

خسارات از این دست می‌باشند. این فرآیند در زمان اجرا دارای نقاط تصمیم گیری کنترل شده (مانند نقطه برگشت یا پایان عملیات) است. موفقیت در تاثیرگذاری بر تصمیم گیری‌های نفوذگر در این نقاط کلیدی می‌تواند نتیجه خوبی برای مدافع داشته باشد. به مجموعه اقدامات بازدارنده، رفع کننده، دفع کننده و بازیابی کننده به منظور پیشگیری، حفظ، حمایت از ارزش‌ها، منافع و دارایی‌های ملی در مقابل تهدیدات و حملات سایبری انجام می‌گیرد، دفاع سایبری می‌گویند[۳]. البته این تعریف حاوی معیارهای پیش‌کنشگرانه[۳] مربوط به دفاع سایبری فعال[۴] نیز می‌باشد. تعریف دفاع سایبری قبل از ورود مفهوم دفاع سایبری فعال به عرصه سایبر، به دسته‌ای از اقدامات که به منظور مقابله با آسیب‌های ناشی از رویدادهای سایبری یا بازگردانی کارکرد سیستم‌ها و شبکه‌ها به حداکثر عملکرد ممکن در زمان به وقوع پیوستن یک رویداد به کار می‌روند، گفته می‌شد، که همان تعریف دفاع سایبری غیرفعال می‌باشد. اکثرا دفاع سایبری فعال را در مقابل دفاع سایبری غیر فعال قرار می‌دهند و استفاده از پادآوندها، ضدبدافزارها و فن‌آوری‌های تشخیص بدافزار را دفاع سایبری غیرفعال می‌دانند. اساسا غیرفعال دانستن بقیه رویکردهای دفاعی نادرست است و باید آن را ناشی از نبود تعریف روشن برای آن‌ها دانست. بدین منظور به جای استفاده از عبارت نادرست دفاع سایبری غیرفعال باید از یک دسته بندی دقیق‌تر برای این اقدامات یعنی مفهوم دفاع سایبری مستحکم[۵] و دفاع سایبری تاب‌آور[۶] استفاده شود. دو مفهوم دفاع سایبری مستحکم و دفاع سایبری تاب‌آور به نوعی زیرمجموعه مفهوم دفاع سایبری پیشین بوده و در کنار دفاع سایبری فعال یک سه گانه دفاعی را تشکیل می‌دهند.

یکی از بهترین تعاریف موجود برای دفاع سایبری فعال توسط رابرت دوار[۳] در سال ۲۰۱۴ ارائه شده است. او دفاع سایبری فعال را یک الگوی امنیتی دارای دو مؤلفه زیر بیان می‌کند.

- شناسایی و مقابله برخط با تهدیدات در شبکه‌های مدافعین
- ظرفیت اتخاذ اقدام متقابل تهاجمی و خشن در شبکه خارجی

بنابراین اینگونه دفاع سایبری فعال را تعریف نموده است: "رویکردی به منظور دستیابی به امنیت سایبری مبتنی بر بکارگیری تدابیری برای کشف، شناسایی، تجزیه و تحلیل و مقابله با تهدیدات به صورت برخط از داخل و خارج شبکه‌ها و سیستم‌های ارتباطی، ترکیب شده با توانایی و ابتکار در انجام اقدامات پیش‌کنشگرانه یا تهاجمی در قبال تهدیدات و موجودیت آن‌ها شامل اقداماتی در شبکه‌های خانگی حمله‌کنندگان[۳]."

اطلاعات جزء مهم‌ترین بخش‌های دفاع سایبری فعال بوده و جمع‌آوری اطلاعات به هر طریق و روش ممکن جزء اصلی ترین رکن این نوع دفاع می‌باشد. این جمع آوری اطلاعات از مهاجم به حدی اهمیت دارد که حتی روش حمله متقابل هم در این نوع دفاع سایبری به عنوان یک عامل بازدارنده قوی و ایجاد کننده آگاهی وضعیتی[۷]، مورد بررسی و پیاده‌سازی قرار می‌گیرد. نفوذگر باید در مرحله تجسس و پویش شبکه شکست داده شود و مغلوب گردد، نه در زمانی که حمله را انجام داده است. زیرا حین شناسایی شبکه، نفوذگران به علت نداشتن اطلاعات کافی در مدت زمان طولانی تری در معرض خطر هستند. بدین ترتیب نفوذگران در این زمان بیشتر مستعد آسیب دیدن می‌باشند. دفاع فعال سایبری برای محقق نمودن این منظور از روش‌ها و تکنیک‌های منحصربه فرد مختلفی استفاده می‌کند، که هدف همه آن‌ها جمع آوری اطلاعات و ایجاد یک آگاهی وضعیتی از شبکه خودی، خود مهاجم، روش‌ها، تکنیک‌ها و ابزارهای مورد استفاده او می‌باشد[۶].

طبق گفته اندسلی[۴]، آگاهی وضعیتی به طور ساده این است که بدانید در اطراف شما چه می‌گذرد. تعریفی که وی به این صورت گسترش داده است. "مشاهده عناصر در محیط در یک حجم از زمان و مکان، درک و فهم معنای آن‌ها و پیش بینی وضعیت آن‌ها در آینده نزدیک".

---

۲ Proactive Measures
۳ Active Cyber Defense (ACD)
۴ Fortified Cyber Defense (FCD)
۵ Resilient Cyber Defense (RCD)
۶ Situational Awareness (SA)

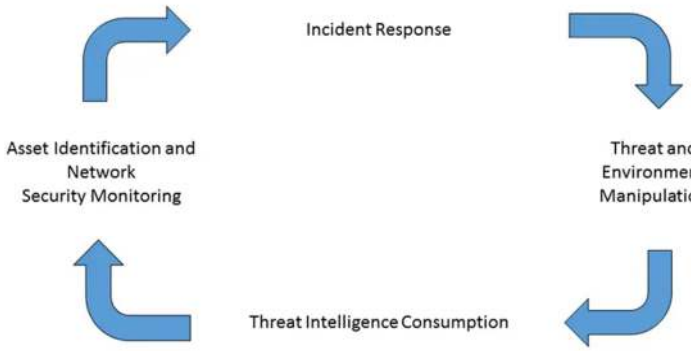
ذکر این نکته ضروریست که کشورهای پیشتاز در عرصه سایبری یک به یک در حال گذار از دفاع سایبری غیر فعال به دفاع سایبری فعال هستند، و برای رسیدن به هدف خود برنامه‌های چند ساله طراحی نموده‌اند. این پژوهش می‌تواند مقدمه‌ای برای ورود جدی‌تر به پیاده‌سازی این نوع دفاع در کشور ایران باشد. در اکثر مقالات داخلی در حوزه دفاع سایبری فعال روی جنبه‌های مفهومی این نوع دفاع تمرکز شده است. مقالات در حوزه آگاهی وضعیتی نیز اکثرا بر پایه دفاع‌های سایبری پیشین بوده و یا صرفا برخی از راهبرهای فعالانه در آن‌ها دیده می‌شود. این در حالیست که کشورهایی مانند آمریکا و انگلیس از مرحله مفهومی، ریاضی و مدل سازی عبور کرده و به محصول استراتژیک رسیده‌اند. در این مقاله ضمن جمع‌آوری تکنیک‌های منحصر به فرد دفاع سایبری فعال و بررسی مهم ترین بخش این نوع دفاع یعنی آگاهی وضعیتی سایبری، بر اثربخشی و بازدارندگی این نوع دفاع تاکید می‌گردد. سپس لزوم ارائه یک مدل گسترده آگاهی وضعیتی بر مبنای راهبردها و تکنیک‌های این نوع دفاع نشان داده می‌شود.

۲- دفاع سایبری فعال

رویکردهای دفاعی پیشین دیگر جوابگوی حملات پیچیده و هوشمند مهاجمان نیستند و همیشه چندین گام از آن‌ها عقب‌تر می‌باشند. به همین علت متخصصان و کارشناسان حوزه سایبری چند سالی است که نظریه یک رویکرد جامع، هوشمند، خودکار و بلادرنگ را مطرح نمودند. این نظریه "دفاع سایبری فعال" نام گرفته است که مهم ترین بخش آن آگاهی وضعیتی می‌باشد. دفاع سایبری فعال مبتنی بر استفاده از ابزارهایی است که نه تنها حوادث سایبری را در هنگام وقوع شناسایی و متوقف می‌کند، بلکه اقدامات تهاجمی را برای به حداقل رساندن قابلیت‌های مهاجمان انجام می‌دهد. علاوه بر این می‌تواند از طریق انواع راه‌های فنی مانند استقرار طعمه یا هک کردن شبکه مهاجم اقداماتی را جهت خنثی سازی فعالیت‌های صورت گرفته انجام دهد[۱]. با توجه به تمامی تعریف‌های موجود برای دفاع سایبری فعال و بررسی و تحلیل‌های انجام گرفته در خصوص این نوع دفاع، تعریف ما اینگونه ارائه می‌گردد: "یک توانایی هماهنگ، خودکار و برخط به منظور کشف، شناسایی و مقابله با تهدیدات قبل از وقوع خسارت با استفاده از یک آگاهی وضعیتی قدرتمند و اشتراک گذاری اطلاعات تهدید بوده که از تمامی ظرفیت‌های دفاع‌های پیشین(پیشگیرانه و تاب‌آور و بازسازی کننده) در کنار تکنیک‌های منحصربه فرد دفاع سایبری فعال شامل توانایی و ابتکار در انجام اقدامات پیش‌کنشگرانه یا تهاجمی با تکیه بر اصل مدیریت خطرپذیری سیستم و محیط، بهره می‌گیرد."

همان‌طور که در شکل(۱) مشخص است، چرخه دفاع سایبری فعال ماموریت یک چرخه فعال دفاع سایبری ادامه دار و بدون توقف را مفهوم‌سازی نموده که شامل چهار فاز (مرحله) می‌باشد:

- شناسایی دارایی‌ها و نظارت بر امنیت شبکه
- واکنش به حوادث
- تهدید و دست کاری محیط
- بهره برداری از اطلاعات تهدید



شکل(۱): چرخه دفاع سایبری فعال[۷]

چرخه دفاع سایبری فعال یک چرخه ادامه دار و بدون حالت پایان می‌باشد. اگرچه همانند یک چرخه‌ای از رخدادهای متوالی معرفی شده است ولی در عمل فازهای چرخه دفاع سایبری فعال، فرآیندهای ادامه داری را نشان می‌دهد که به طور همزمان اتفاق افتاده و به هم وابسته می‌باشند. شناسایی دارایی‌ها و نظارت برامنیت شبکه یک آگاهی وضعیتی قدرتمند از طریق شناخت محیط یک سازمان، شامل یک محاسبه دقیق از تجهیزات شبکه، یک فهم عمیق از معماری شبکه و یک نظارت موثر بر فعالیت‌های شبکه، ایجاد می‌نماید. بهره برداری از اطلاعات تهدید، شناسایی و استفاده از اطلاعات تهدید مناسب برای محیط کاری یک سازمان، دارایی‌های شبکه و معماری آن می‌باشد. واکنش به حوادث، اقدامی است که به منظور مقابله با یک تهدید شناسایی شده در شبکه یک سازمان انجام می‌گیرد. تهدید و دستکاری محیط مشخص می‌نماید چطور یک سازمان انتخاب می‌کند که از طریق تعامل با تهدید، اطلاعات بیشتری از آن بدست آورد یا از طریق دستکاری محیط با تهدید مقابله نماید. این شامل اقداماتی از قبیل تجزیه و تحلیل ایستا و پویای بدافزارها و ایجاد تغییرات فیزیکی یا منطقی در معماری شبکه باشد.

آمریکا و انگلستان به عنوان دو قدرت سایبری مدل‌های دفاع سایبری فعال بومی را طراحی نموده و توسعه داده‌اند. مرکز دارپای[۸] ایالات متحده آمریکا در سال ۲۰۱۵ راهبرد دفاع سایبری فعال را با ارائه مدل شارکسیر[۹] پیاده سازی نمود[۸]، که می‌تواند در مقابل حملات صفر روزه[۱۰] نیز مقاومت نماید. مرکز ملی امنیت سایبری انگلستان نیز در سال ۲۰۱۶[۹]، راهبرد پنج ساله‌ای برای تحقق و پیاده سازی دفاع سایبری فعال در کشور خود ارائه داده است. همه این‌ها نشان دهنده اهمیت دفاع سایبری فعال و لزوم حرکت جمهوری اسلامی ایران به سمت پیاده‌سازی مدل‌های بومی این نوع دفاع می‌باشد.

۱-۲- تکنیک‌های اختصاصی ACD[۱۱]

از گزینه‌های دفاعی نسبتاً متداول و کم‌خطر دفاع سایبری فعال می‌توان از به اشتراک گذاری اطلاعات و استفاده از تله عسل یا تارپیت[۱۲] نام برد. یک متخصص امنیت رایانه که از یک تله عسل در شبکه خود استفاده می‌کند، می‌تواند با فرض اینکه این سیستم مهاجم را فریب می‌دهد، تکنیک‌های حمله مهاجم را مشاهده کرده و از این مشاهدات برای اطلاع دفاع در شبکه واقعی مدافع استفاده نماید.

تکنیک انکار و فریب سایبری یکی دیگر از روش‌های دفاعی کم خطر است که می‌تواند برای مشاهده رفتار مهاجم، طراحی سایر تکنیک‌های دفاعی فعال و بهبود قابلیت پاسخ به حوادث مورد استفاده قرار گیرد. این تکنیک توانایی پنهان سازی اطلاعات واقعی و آشکارسازی اطلاعات غلط را داشته تا درک متجاوز از اطلاعات موجود در یک سیستم رایانه‌ای، آسیب پذیری‌های آن سیستم و دفاع‌های مستقر در شبکه را مختل کند. فرآیند شکار مهاجمان در شبکه، بیرون کردن مهاجمین در صورت دور زدن اقدامات غیرفعال دفاعی و ورود به شبکه مدافع می‌باشد. شکار مهاجمین به همان اندازه که به منظور از بین بردن تهدیدها بوده، شناسایی روش‌ها و واکنش‌های قابل اجرای آنان را نیز در نظر می‌گیرد و به افشای آن‌ها نیز می‌پردازد. تکنیک‌هایی مانند دیده‌بان شبکه با مشاهده کل رویدادهای شبکه و جابه جایی آدرس شبکه به منظور ارسال ترافیک مشکوک به سرورهای از پیش تعیین شده جهت ارزیابی می‌توانند اطلاعاتی در مورد حملات احتمالی بدست آورند[۵و۶].

همچنین استفاده از کرم‌های سفید، به عنوان نوعی نرم افزارهای بی‌خطر شبیه ویروس‌ها که وظیفه جستجو و نابود ساختن نرم افزارهای مخرب، تشخیص تجاوز و همچنین ایفای نقش در شیوه‌های بازیابی را دارند، یکی دیگر از تکنیک‌های موثر این نوع دفاع هستند[۳].

---

[۷] The Defense Advanced Research Projects Agency
[۸] sharkseer
[۹] Zero-day Attack
[۱۰] Active Cyber Defense
[۱۱] Honeypot or Tarpits

برخی از تکنیک‌های دفاع فعال، فعالیت‌هایی هستند که مخاطره بیشتری دارند، زیرا عموماً شامل عملیات خارج از شبکه شخص بوده و در صورت استفاده بدون دقت لازم، می‌تواند منجر به آسیب‌های جانبی جزئی یا نگرانی‌های مربوط به حریم خصوصی شوند. این فعالیت‌ها شامل استفاده از بیکن‌ها[۱۲] و جمع آوری اطلاعات در وب عمیق و وب تاریک است. بیکن‌ها قطعاتی از کد هستند که در پرونده‌هایی که حاوی اطلاعات حساس هستند، جاسازی شده‌اند. آن‌ها را می‌توان به دو طریق عملیاتی کرد. اولاً، بیکن‌هایی با مخاطره پایین که اگر یک موجودیت غیرمجاز بخواهد فایلی را از شبکه خانگی حذف کند، به صاحب آن هشدار می‌دهند و به عنوان یک زنگ هشدار داخلی عمل می‌کند. دوم، بیکن‌هایی تهاجمی‌تر برای بازگرداندن اطلاعات قربانی از میان آدرس‌های اینترنتی و پیکربندی شبکه سیستم‌های رایانه‌ای که یک سند سرقت شده از طریق آن‌ها هدایت می‌شود، طراحی شده‌اند.

مدافعان شبکه به طور فزاینده‌ای متوجه این امر خواهند شد که اطلاعاتی که از طریق شبکه تاریک عبور می‌کند توانایی این را دارد که برای اطلاع از راهبردهای دفاعی و هشدار مقامات امنیتی، به اطلاعات در مورد یک آسیب پذیری کمک کننده باشد. در این قلمرو از اینترنت که در آن وب سایت‌ها از سرورهای قابل ردیابی جدا شده‌اند، ناشناس بودن کاربران رایج است و اطلاعات آنان بین شبکه‌های معتبر و گروه‌های امن هدایت می‌شود. این شبکه در تجارت مجرمانه اطلاعات سرقت شده و خدمات بدافزارها رایج بوده و از این رو امکانات اطلاعاتی مناسبی برای مدافعان شبکه فراهم می‌نماید.

به عنوان مثال، تیم امنیتی یک بانک می‌تواند در بازارهای غیرقانونی جستجو کرده و اطلاعات شخصی یا مالی برای فروش را با اطلاعاتی که بانک در مورد مشتریان و حساب‌های آن‌ها حفظ می‌کند مقایسه کند. اگر تیم امنیتی این مورد مهم را کشف کند، به احتمال زیاد یک نفوذگر شبکه آن‌ها را نقض کرده و بدون ایجاد زنگ هشدار، داده‌های حساس را با موفقیت سرقت کرده است. مدافعان، که اکنون از وجود آسیب پذیری شبکه آگاه شده‌اند، می‌توانند به دنبال تقویت شکاف در معماری امنیتی خود باشند و پیش از به خطر انداختن اطلاعات بیشتر، نفوذگران را از سیستم و شبکه خود دور کنند.

از دیگر اقدامات دفاع فعال که بیشتر تهاجمی و خطرناک هستند، شامل باج افزارهای کلاه سفید[۱۳] و ماموریت نجات، اغلب مورد توصیه برای اطلاعاتی هستند که قبلاً از شبکه شخصی سرقت شده است. در حالی که استفاده مخرب از باج افزار در سال‌های گذشته به یکی از نگران‌کننده‌ترین موضوعات امنیت سایبری تبدیل شده است، کارشناسان امنیتی امکان استفاده از ابزارهای مشابه برای رمزگذاری داده‌های سرقت شده که در حال انتقال در شبکه سوم هستند را در نظر گرفته‌اند. به این ترتیب، آن‌ها می‌توانند به شخص سوم اطلاع دهند که نفوذگران شبکه آن‌ها را به خطر انداخته و از آن برای انتقال داده‌های سرقت شده استفاده می‌کنند. باج افزار کلاه سفید به مدیران شبکه اطلاع می‌دهد و می‌تواند اطلاعات سرقت شده را بازیابی کرده و سپس باج‌افزار را از رایانه‌های طرف سوم حذف کند.[۵و۱۷].

استفاده از تکنیک‌های منحصربه فرد ACD مانند هک متقابل[۱۴] یعنی نفوذ در شبکه مهاجم به منظور(شناسایی هویت حمله کننده، شناسایی تکنیک‌های حمله و روش ها و ابزارهای وی و برگرداندن یا پاک نمودن داده‌های به سرقت رفته از سیستم وی) برای نفوذگران مشکلات زیر را ایجاد نموده که خود نوعی بازدارندگی برای محیط و سیستم و زیرساخت ما ایجاد می‌کند[۶].

- غیرقابل پیش بینی بودن
- تردید و بلاتکلیفی نفوذگر
- افزایش هزینه منابع مصرفی نفوذگر
- افزایش مخاطره برای نفوذگر

[۱۲] Beacons
[۱۳] White-Hat Ransomware
[۱۴] Hack-back

۳- آگاهی وضعیتی سایبری

آگاهی وضعیتی به عنوان حالتی از آگاهی نسبت به شرایطی که در اطراف ما وجود دارد، به ویژه شرایطی که مربوط به ما بوده و ما به آن‌ها علاقه مند هستیم، تعریف می‌شود. مدل اندسلی به عنوان یک مدل مرجع در آگاهی وضعیتی سایبری بوده و سایر مدل‌های آگاهی وضعیتی بر پایه آن توسعه داده شده‌اند. آگاهی وضعیتی توسط اندسلی به صورت زیر تعریف شده است: "آگاهی وضعیتی، درک یک عناصر محیط در یک زمان و مکان مشخص، شناخت معنای آن‌ها، و پردازش وضعیت آن‌ها در آینده نزدیک است[۴]". یک مدل آگاهی وضعیتی سایبری کامل باید روی پیشگیری، یعنی پیاده‌سازی یک سیستم هشدار زودهنگام که می‌تواند حوادث ملی را پیشگیری و شناسایی کند، تمرکز نماید[۱۰].

بر مبنای تعریف آگاهی وضعیتی ارائه شده توسط اندسلی، تشکیل آگاهی وضعیتی شامل سه سطح است.

سطح ۱: مشاهده عناصرها در محیط، اولین قدم در دستیابی به آگاهی وضعیتی است. این سطح، مشاهده وضعیت، ویژگی‌ها، و دینامیک های عناصر مرتبط در محیط را پوشش می‌دهد.

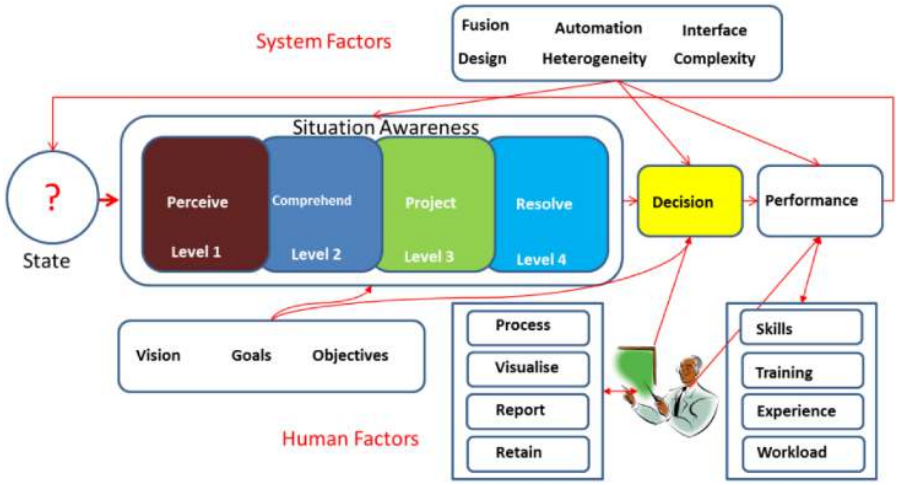
سطح ۲: فهم وضعیت کنونی بر مبنای خروجی سطح(۱) انجام می‌شود. این سطح شامل شناخت اهمیت عناصر مرتبط است.

سطح ۳: تجسم وضعیت‌های آتی، قابلیت پیش‌بینی کنش‌های آینده عناصر در محیط را پوشش می‌دهد. این موضوع با اطلاعات وضعیت و دینامیک عناصر و فهم وضعیت انجام می‌شود.

همان‌طور که در شکل(۲) مشخص است فوی و مک گینس[۱۱] از مدل آگاهی وضعیتی اندسلی استفاده نموده و مرحله پیشنهاد را به عنوان مؤلفه چهارم اضافه کرده‌اند، که بعدها توسط اونووبیکو[۱۲] پالایش شده ااین اصطلاحات (مشاهده، درک، پیش بینی و پیشنهاد) و ارتباط آن‌ها با فضای سایبر بررسی شده است. مشاهده با جمع آوری شواهد از وضعیت‌های سایبری سروکار دارد، درک مربوط به فهم دقیق وضعیت بوده که ممکن است از تجزیه و تحلیل مجموعه‌ای از شواهد جمع آوری شده یا از وضعیت فعلی فضای سایبر حاصل شود، همچنین شامل درک دقیق سطح تهدید است. شناسایی انواع حمله و خطرات مرتبط یا وابسته به یکدیگر از دیگر وظایف این مرحله می‌باشد. مرحله تجسم با اقدامات پیش بینی کننده به منظور پیش بینی حوادث، شرایط یا وضعیت‌های آینده با استفاده از اطلاعات وضعیت فعلی و درک چگونگی تشدید شرایط فعلی سروکار دارد. سرانجام، مرحله پیشنهاد با کنترل‌هایی برای ترمیم، بازیابی، اصلاح و پاسخ به وضعیت‌های سایبری شناخته می‌شود.

مرحله تصمیم گیری ورودی‌های چند بعدی را به منظور توصیه مجموعه‌ای از اقدامات انجام می‌دهند. برای این امر از فاکتورهای سیستم استفاده می‌کنند و شواهد نتیجه تجزیه و تحلیل داده‌های اطلاعات تهدید را با در نظر گرفتن چشم انداز، اهداف و اهداف کسب و کار در نظر می‌گیرند. بعلاوه، مرحله تصمیم از گزارش‌های ارائه شده توسط کارشناسان یا متصدیان برای تصمیم گیری در مورد مناسب‌ترین اقدام جهت رسیدگی به وضعیت یا شرایط استفاده می‌کند. در مدل اندسلی تصمیمات به شدت تحت تاثیر آگاهی وضعیتی قرار می‌گیرند، زیرا آگاهی وضعیتی، داده ورودی غالب در تصمیم گیری است. تصمیمات از فاکتورهای متنوع، مانند فاکتورهای فردی(تجربه یا قابلیت‌ها) یا از فاکتورهای وظیفه و محیطی(حجم کاری، فشارها یا پیچیدگی‌ها) تاثیر می‌گیرد. در این مدل می‌توان ارتباط بین آگاهی وضعیتی و عملکرد کنش‌ها را پیش‌بینی کرد[۴]. آگاهی وضعیتی مناسب، احتمال عملکرد خوب و کنش‌های دقیق را افزایش می‌دهد، اما نمی‌تواند آن را تضمین کند. همچنین بازخورد، وضعیت محیط یا سیستم تحت تاثیر تصمیمات و عملکرد کنش‌های انتخابی را پوشش می‌دهد.

در مدل آگاهی وضعیتی، زمان یک نقش مهم ایفا می‌کند. آگاهی وضعیتی یک ساختار دینامیک متاثر از محیط بیرونی و فاکتورهای متعدد است و در مدل، به عنوان ورودی عمل می‌کند. آگاهی وضعیتی سایبری موثر مستلزم این است که آگاهی وضعیتی سایبری ایجاد شده توسط سیستم، هوشمندی بهتری در خصوص وضعیت شبکه به تحلیلگرها ارائه کند[۱۴].



شکل(۲): مدل مرجع آگاهی وضعیتی[۱۳]

۱-۳- کارهای مرتبط

با وجود بازه گسترده کاربرد آگاهی وضعیتی، اغلب مدل‌های دستیابی به SA[۱۶] یک شباهت دارند: آن‌ها مبتنی بر تعریف کلی و رایج‌ترین مدل SA یعنی اندسلی[۴] هستند. بنابراین، اجزای توصیف شده توسط اندسلی با ترکیب تمامی مدل‌های مناسب موجود، به عنوان پایه‌ای برای ایجاد یک فرآیند جدید برای دستیابی و اعمال SA عمل می‌کنند.

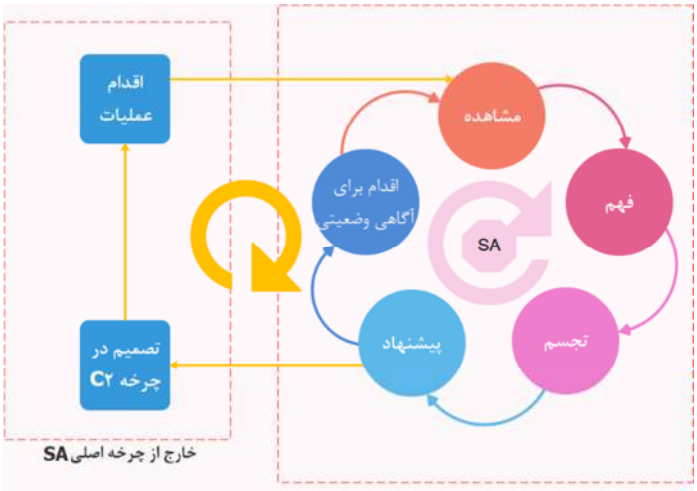
تمامی مدل‌های موجود در فرآیند دستیابی به آگاهی وضعیتی سه مرحله (مشاهده، درک و پیش بینی) را پوشش می‌دهند. (به عنوان مثال مرحله مشاهده و درک در مدل اندسلی یا مرحله مشاهده و جهت‌گیری در حلقه اوودا[۱۷]). البته مدل‌های اندسلی و اوودا[۱۹] بر خلاف مدل‌های دیگر بر اساس مهارت‌های شناختی متصدی های انسانی عمل می‌نمایند و سایر مدل‌ها از فرآیندهایی که توسط ماشین‌ها انجام شده بهره می‌گیرند. در خصوص فرآیندهای کاربردی SA که شامل (پیش‌بینی و پیشنهاد، اقدام و بازخورد) بوده مدل‌ها وضعیت متفاوتی از خود به نمایش می‌گذارند. مدل‌های اندسلی، اوودا، اوانکیچ[۱۴] و پاهی[۱۰] مرحله پیشنهاد را به صورت جامع‌تر توصیف می‌کنند و مدل‌های ادغام اطلاعات استینبرگ[۱۸]، مدل مرجع تادا و سالیرنو[۱۵] و همچنین مدل اوکولیکا[۱۶] با فراهم نمودن اطلاعات بهتر و دقیق فرآیند پیشنهاد و تصمیم گیری را ارتقا می‌دهند. برای مثال مدل اوودا مراحل مورد نیاز برای پیشنهاد را به صورت مفصل توصیف می‌کند، در حالی که مدل اوانکیچ ویژگی‌های فنی مورد نیاز برای پیشنهاد با پیش‌بینی سناریوهای احتمالی را فراهم می‌نماید. به طور ایده‌آل، فرآیند دستیابی به SA شامل یک چرخه بازخورد بین محیط و تصمیم‌گیر است. برای مثال متصدی می‌تواند فرآیندهای دستیابی به SA و نتایج آن‌ها را تایید یا اصلاح کند.

از جنبه متصدی، هدف از تحلیل، ارزیابی چگونگی رسیدن به SA توسط انسان‌ها یا ماشین‌ها (مانند برنامه‌ها) در مدل‌های SA است. مدل‌های اول، مانند اندسلی و حلقه اوودا، روی جنبه انسانی در شرایط بحرانی تمرکز می‌کنند. آن‌ها SA را به عنوان یک دانش شناختی توصیف نموده، که می‌توان با تجربه آن را غنی کرد. در این مدل‌ها، متصدی یک انسان، مانند یک خلبان یا یک سرباز است. حسگرهای فنی و داده‌های آن‌ها مشاهده انسانی را تکمیل می‌کنند. به عنوان نمونه رویکرد مدل ادغام داده نیاز به فرآیندهای اطلاعاتی انسانی و ماشینی در دستیابی به SA و کاربرد آن را بیان می‌کند. همه مدل‌های آگاهی وضعیتی بیان شده تلاش می‌کنند تا فرآیندهای دستیابی به SA شناختی را با ترکیب راه حل‌های فنی بهبود دهند. مدل‌های دیگر، مانند آگاهی

[۱۵] Situational Awareness
[۱۶] ooda

وضعیتی سایبری موثر اوانکیچ و مدل مرجع آگاهی وضعیتی، رویکرد متفاوتی دارند. آن‌ها در فرآیندهای ایجاد SA، از متصدی انسانی در نقش تاییدکننده یا بهبود دهنده استفاده می‌کنند، در حالی که فرآیندهای دستیابی به SA کاملا خودکار است[۱۰].

در این بین مدل دفاع فعال سادک[۱۸][۲] شکل(۳) از پنج مرحله (مشاهده، فهم، تجسم، پیشنهاد و اقدام برای آگاهی وضعیتی) تشکیل شده است. این مدل تمام ویژگی‌های مدل‌های پیشین را دارا بوده و به صورت یک چرخه فعال مفاهیم فعالانه و خودکارسازی اقدامات را به صورت مفهومی نشان می‌دهد. در این مدل دفاع فعال، آگاهی وضعیتی به صورت یک چرخه فعال عمل نموده و در بخش اقدام برای آگاهی وضعیتی، اقدامات مورد نیاز را داخل همین چرخه انجام می‌دهد. این موضوع موجب افزایش سرعت اقدامات آگاهی وضعیتی و به تبع آن سرعت تصمیم گیری در سیستم می‌گردد. همچنین سایر اقدامات (از نوع عملیاتی) نیز جهت تصمیم گیری متصدی به خارج از این چرخه منتقل می‌شود.



شکل(۳): مدل مفهومی دفاع فعال سادک[۲]

نقطه ضعف مشترک همه مدل‌های آگاهی وضعیتی در عدم بهره‌گیری حداکثری از مفاهیم و چهارچوب دفاع سایبری فعال و تکنیک‌های آن، بوده است. در همه مدل‌های آگاهی وضعیتی مذکور پیشنهادات برای تصمیم گیری نهایی به متصدی امنیتی سپرده شده که این موضوع چابکی و برخط بودن اقدامات سیستم را با مشکل مواجه می‌نماید. دخالت عامل انسانی در اتخاذ همه تصمیمات با مخاطره بالا یا پایین موجب می‌گردد آگاهی وضعیتی ایجاد شده نتواند در زمان مقرر به تهدیدات پاسخ دهد. در تمامی این مدل‌ها به موضوع سرعت و دقت در تصمیم گیری به طور جدی پرداخته نشده و به نظر تمامی این مدل‌ها برای چهارچوب دفاع‌های سایبری پیشین طراحی شده‌اند. نبود یک بخش مدیریت مخاطره به منظور اتخاذ برخی از اقدامات عملیاتی توسط خود سیستم آگاهی وضعیتی برای افزایش مؤلفه فعالانه و خودکار بودن، یکی دیگر از ضعف‌های این مدل‌ها می‌باشد.

مدل مفهومی سادک تنها مدلی است که بر مبنای چهارچوب دفاع سایبری فعال طراحی شده و اقدامات فعالانه و خودکار در آن دیده شده است. تکمیل این مدل نیاز به طراحی یک مدل گسترده با مشخص نمودن همه زیرشاخه‌ها و بخش‌های یک آگاهی وضعیتی در دفاع سایبری فعال خواهد داشت.

۴- نتیجه‌گیری

دفاع سایبری فعال یک توانایی هماهنگ، خودکار و برخط به منظور کشف، شناسایی و مقابله با تهدیدات قبل از وقوع خسارت با استفاده از یک آگاهی وضعیتی قدرتمند و اشتراک گذاری اطلاعات تهدید است، که از تمامی ظرفیت‌های دفاع‌های پیشین

[۱۷] Situational Awareness Decision Action (SADAC)

(پیشگیرانه و تاب‌آور و بازسازی کننده) در کنار تکنیک‌های منحصربه فرد دفاع سایبری فعال شامل توانایی و ابتکار در انجام اقدامات پیش‌کنشگرانه یا تهاجمی با تکیه بر اصل مدیریت خطرپذیری سیستم و محیط، می‌باشد. آگاهی وضعیتی همواره جزء اصلی و غیرقابل انکار این نوع دفاع بوده و مدل‌های ارائه شده قبلی نیز با وجود عدم اشاره ظاهری به دفاع فعال در ارائه مدل‌های آگاهی وضعیتی ارائه شده، در مفهوم به برخی از مؤلفه‌های دفاع سایبری فعال اشاره می‌کنند.

مدل سادک به عنوان یک مدل دفاع فعال و در برگیرنده یک چرخه فعال آگاهی وضعیتی می‌باشد. تکمیل این مدل نیاز به طراحی یک مدل گسترده با مشخص نمودن همه زیرشاخه‌ها و بخش‌های یک آگاهی وضعیتی در دفاع سایبری فعال خواهد داشت. مدل گسترده‌ای که براساس مفاهیم و چهارچوب دفاع سایبری فعال بوده و تمامی تکنیک‌های منحصربه فرد این نوع دفاع سایبری را بکار گرفته باشد. در این مقاله ضمن ارائه یک تعریف جدید از دفاع سایبری فعال و جمع‌آوری تکنیک‌های منحصر به فرد آن، بر اثربخشی و بازدارندگی این نوع دفاع تاکید شد. همچنین با بررسی برخی از ابعاد دفاع سایبری فعال و بخش اساسی آن یعنی آگاهی وضعیتی سایبری، لزوم ارائه یک مدل گسترده آگاهی وضعیتی بر مبنای راهبردها و تکنیک‌های این نوع دفاع نشان داده شد.

ارایه یک مدل گسترده آگاهی وضعیتی در دفاع سایبری فعال و ارزیابی آن، همچنین یک مدل ریاضی جامع که در برگیرنده تمامی جوانب و بخش‌های عملکردی مدل آگاهی وضعیتی در دفاع سایبری فعال باشد، به همراه یک بستر نرم‌افزاری برای شبیه سازی، می‌توانند به عنوان پیشنهاداتی برای کارهای آینده مورد بررسی قرار گیرند.

مراجع

[۱] تبار احمدی، داداش و بابویی، محمود، (۱۴۰۰). *ارائه مدلی برای دفاع سایبری فعال به منظور کاربرد در فناوری فریب سایبری*. پدافند الکترونیکی و سایبری، ۹(۴)، ۱۲۵-۱۴۰.

[۲] رشیدی، علی جبار، (۱۳۹۹). *آگاهی وضعیتی سایبری*. گزارش فنی، دانشگاه صنعتی مالک اشتر.

[3] R. S. Dewar, "*The "triptych of cyber security": A classifi cation of active cyber defence*," in *2014 6th International Conference On Cyber Conflict (CyCon 2014)*, pp. 7-21: IEEE, 2014.

[4] M. R. Endsley, "*Toward a theory of situation awareness in dynamic systems*," Human factors, vol. 37, no. 1, pp. 32-64, 1995.

[5] D. C. Blair, M. Chertoff, F. J. Cilluffo, and N. O'Connor, "*Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats*," Project Report, The George Washington University, 2016.

[6] K. A. Repik, "*Defeating adversary network intelligence efforts with active cyber defense techniques*," 2008.

[7] Mandt, Erick J. "*On integrating cyber intelligence analysis and active cyber defense operations*." PhD diss., Utica College, 2015.

[8]Active Cyber Defense System. Available: *https://www.iad.gov/iad/programs/iad-initiatives/active-cyber-defense.cfm*. 2017.

[9] Levy, Ian, S. Maddy, and Mission Analytics. "*Active Cyber Defence-The Second Year*." 2019.

[10] T. Pahi, M. Leitner, and F. Skopik, "*Analysis and assessment of situational awareness models for national cyber security centers*," in International Conference on Information Systems Security and Privacy, vol. 2, pp. 334-345: SCITEPRESS, 2017.

[11] B. McGuinness and L. Foy, "*A subjective measure of SA: the Crew Awareness Rating Scale (CARS)*," in Proceedings of the first human performance, situation awareness, and automation conference, Savannah, Georgia, vol. 16, pp. 286-291, 2000.

[12] C. Onwubiko, *Situational Awareness in Computer Network Defense: Principles, Methods and Applications: Principles, Methods and Applications*. IGI Global, 2012.

[13] C. Onwubiko, "*Understanding Cyber Situation Awareness*," Int. J. Cyber Situational Aware., vol. 1, no. 1, pp. 11-30, 2016.

[14] N. Evancich, Z. Lu, J. Li, Y. Cheng, J. Tuttle, and P. Xie, *"Network-wide awareness," in Cyber Defense and Situational Awareness*: Springer, pp. 63-91, 2014.

[15] Tadda, George P., and John S. Salerno. "*Overview of cyber situation awareness." In Cyber situational awareness*, pp. 15-35. Springer, Boston, MA, 2010.

[16] Okolica, James, J. Todd McDonald, Gilbert L. Peterson, Robert F. Mills, and Michael W. Haas. "*Developing systems for cyber situational awareness*." In 2nd Cyberspace Research Workshop, vol. 46. 2009.

[17] Broeders, Dennis. "*Private active cyber defense and (international) cyber security—pushing the line?*." Journal of Cybersecurity 7, no. 1 2021.

[18] A. Steinberg, C. Bowman, and F. White, "*Revisions to the JDL Model: Joint NATO,*" in IRIS Conference Proceedings, Quebec, October, 1998.

[19] B. Brehmer, "*The dynamic OODA loop: A new basis for designing C2 support*," in Proceedings of the Second International Conference on Military Technology, Stockholm Obtober, 2005, vol. 25, p. 2005.