همایش پژوهش‌های نوین در علوم و فناوری
Conference on Recent Research in Science and Technology

بهره‌گیری از چارچوب کانوین در مواجهه با پویایی و پیچیدگی امنیت فضای سایبر

***محمد عابدی[۱]، محمدرضا کریمی قهرودی[۲]**

[۱] دانشجوی دکتری مدیریت راهبردی فضای سایبر، گرایش امنیت سایبر، دانشکده امنیت ملی، دانشگاه عالی دفاع ملی، تهران، ایران
m.abedi@sndu.ac.ir

[۲] استادیار و عضو هیأت علمی دانشگاه صنعتی مالک اشتر
favad110@gmail.com

چکیده

تصمیم‌گیری در محیط‌های پویا و پیچیده همچون فضای سایبر که همراه با تغییرات سریع و دگرگونی‌های زیاد دارای ریسک بالایی می‌باشد. متأسفانه اکثر تحقیقات در زمینه آگاهی وضعیتی سایبر با تمرکز بر فناوری صورت گرفته است و توجه زیادی به تصمیم‌گیری‌های مبتنی بر انسان نشده است. در حالیکه در وضعیت‌های بحرانی مانند حملات بلادرنگ نیازمند دخالت‌های انسانی در تصمیم‌گیری می‌باشند. به همین دلیل متخصصان و مدیران حوزه امنیت سایبر نیازمند مدل و یا چارچوبی برای تصمیم‌گیری متناسب با هر یک از وضعیت‌های بوجود آمده ناشی از بحران‌های امنیت سایبری می‌باشند. در این پژوهش به معرفی چارچوب کانوین و نحوه بکارگیری آن برای تصمیم‌گیری صحیح در مواجهه با وضعیت‌های گوناگون ناشی از یک حمله سایبری برای کاهش ریسک خواهیم پرداخت. ضمن نگاشت وضعیت‌های ناشی از حمله سایبری در قالب سناریوی فرضی بر دامنه‌های پنج‌گانه چارچوب کانوین اعم از اختلال، آشکار، بغرنج، پیچیده و آشوب، ما در نهایت نشان خواهیم داد که چارچوب کانوین چگونه به متخصصان و مدیران امکان تشخیص وضعیت فعلی و همچنین پاسخ مناسب در شرایط پیچیده بر اساس رابطه علت و اثر را می‌دهد.

کلمات کلیدی: چارچوب کانوین، امنیت فضای سایبر، پیچیدگی، سیستم‌های پیچیده انطباقی، تصمیم‌گیری

۱. مقدمه

پویایی در سیستم‌ها حاکی از وضعیتی است که حالت سیستم در هر لحظه از زمان متناسب با تغییرات عناصر داخلی سیستم و برهم‌کنش آن با عناصر محیطی تغییر می‌کند. در واقع در هر زمان معین، یک سیستم پویا، یک حالت متفاوت از زمان‌های دیگر ممکن است داشته باشد. از طرفی به سیستم‌هایی پیچیده گفته می‌شود که دارای اجزای کوچکتری از کل هستند و با یکدیگر و پدیده‌های خارج از سیستم برهم‌کنش‌هایی دارند و به این علت پیچیدگی را خلق می‌کنند. به عبارتی رفتارهایی از خود بروز می‌دهند که از رفتار اجزاء به تنهایی قابل استنتاج نیست و برای فهم این رفتار به جای بررسی رفتار جداگانه اجزاء، نیاز به نگاهی کل‌نگرانه به جای نگاه کلاسیک گذشته می‌باشد.

در واقع یک سیستم پیچیده، سیستمی است که در آن قسمت‌های گوناگون و تعاملات آن‌ها با یکدیگر رفتارهای خاص را شکل می‌دهند که نمی‌توان آن را با تجزیه و تحلیل اجزای تشکیل‌دهنده آن توضیح داد و نگاهی به کل سیستم باید داشت. در این نوع سیستم‌ها علت و معلول نمی‌توانند لزوماً با یکدیگر مرتبط باشند و در واقع دارای روابط غیرخطی هستند. یک تغییر کوچک می‌تواند تاثیر نامناسبی را در کل رفتار سیستم ایجاد کند(Gandhi, 2014). یک سیستم ترافیکی مثال خوبی برای این نوع

سیستم‌ها می‌باشد در این نمونه تجزیه و تحلیل اتومبیل‌های شخصی و رانندگان خودرو بطور جداگانه کمکی به فهم الگو و دلیل ظهور و بروز تراکم ترافیکی نخواهد کرد.

به عنوان مثالی ملموس‌تر، در اغلب سازمان‌ها تدابیر دفاع چند لایه برای سیستم‌های بحرانی(لایه ای از فایروال ها، سیستم‌های تشخیص نفوذ، مستحکم‌سازی[1] سیستم‌های عامل، احراز هویت قوی و ...) انجام می‌گیرد امّا علیرغم این تلاش‌ها و اقدامات باز هم حمله سایبری اتفاق می‌افتد.

دلیل آن، این است که بررسی جزء به جزء شرایط و اقدامات به طور مستقل از یکدیگر در فرآیند نفوذ حاکی از نفوذ نیست در حالیکه «کل» شرایط و اقدامات هکرها به شکل مجموعه‌ای به هم وابسته موجب بروز خطر و نفوذ در سیستم شده است.

به طور کلی تقلیل‌گرایی[2] و انسجام‌گرایی[3] دو رویکرد متفاوت فلسفی برای تجزیه و تحلیل و طراحی هر شیء یا سیستم هستند. تقلیل‌گرایی استدلال می‌کند که هر سیستم را می‌توان به اجزای کوچکتر آن کاهش داد و سپس عناصر تشکیل دهنده آن را تجزیه و تحلیل کرد در حالی که کل‌گرایان استدلال می‌کنند که کل سیستم بیشتر از مجموع آن است بنابراین یک سیستم را نمی‌توان صرفاً با درک بخش‌های آن تحلیل کرد(McLeod, 2008). اکثر علوم مدرن و روش‌های تحلیل مبنی بر رویکرد تقلیل‌گرایانه است و به خوبی برای درک رفتار یک ساعت مچی، یک ماشین با فضای افلاکی[4] کار می‌کند.

تقلیل‌گرایی تاکید بسیاری روی علیت دارد یعنی تاثیر یک علت منجر به بروز یک معلولی شده است. هنگامی که با سیستم‌های تکوینی مانند رفتارهای انسان، سیستم‌های اقتصادی- اجتماعی، سیستم‌های بیولوژیکی یا سیستم‌های اجتماعی-سایبری مواجه می‌شویم، دیگر رویکرد تقلیل‌گرایی دارای محدودیت‌هایی برای تجزیه و تحلیل می‌باشد، بدن انسان، واکنش جمعی از انسان‌ها به یک محرک سیاسی، واکنش بازارهای مالی برای ادغام شدن در هم و یا تراکم ترافیکی را نمی‌توان از طریق مطالعه اجزای تشکیل‌دهنده آن‌ها پیش‌بینی کرد(Gandhi, 2014).

از نگاه کل‌نگرانه به فضای سایر به عنوان یک سیستم برمی‌آید که این سیستم دارای هر دو ویژگی پیچیدگی[5] و پویایی[6] می‌باشد. پرواضح است که پیچیدگی به نوعی مستتر در ویژگی پویایی می‌باشد چراکه که پویایی سیستم‌ها به نوعی خالق رفتارهای پیچیده می‌باشد. می‌توان با بررسی تحقیقات نوین در حوزه سایبر به عنوان یک سیستم پویا و پیچیده نوعی انطباق برای تداوم کسب و کار و خدمات را ضروری دانست.

سیستم‌های پیچیده انطباقی[7] دارای ویژگی خودآموزی، تکوین و تکامل عناصر تشکیل دهنده سیستم‌های پیچیده نیز می باشند. ویژگی‌های کلیدی سیستم‌های پیچیده انطباقی به شرح ذیل می‌باشند:

- رفتار و یا خروجی را نمی‌توان به سادگی با تجزیه و تحلیل عناصر و ورودی‌های سیستم پیش‌بینی کرد.
- رفتار سیستم در حال تکوین است و با گذشت زمان تغییر می‌کند. تضمینی نیست که به ازای ورودی‌های یکسان، خروجی‌های یکسان نیز داشته باشیم.
- عناصر شرکت‌کننده سیستم خودآموز هستند و رفتار خود را براساس نتیجه تجربیات قبلی تغییر می‌دهند.

لذا با عنایت به تحقیقات گسترده و مدل‌ها و راهکارهای ارائه شده برای تصمیم‌گیری در محیط‌های مبتنی بر ساختارهای سیستم‌های پیچیده انطباقی می‌توان نتیجه گرفت که بررسی فضای سایبر به عنوان یک سیستم پیچیده انطباقی جهت مواجهه صحیح و تسهیل در تصمیم‌گیری، کمک شایانی برای حل مسائل در شرایط گوناگون فضای سایر به ویژه مسائل امنیتی فضای سایبر خواهد کرد. در نتیجه تصمیم‌گیری و حل مسائل در فضای سایبر به ویژه مسائل امنیتی آن که دارای شرایطی پویا و حاصل کل رفتارها و اقدامات می‌باشد نیازمند مدل یا چارچوبی است که ریسک‌های حاصل از تصمیم‌گیری در این محیط پیچیده را

[1] Hardening
[2] Reductionism
[3] Holism
[4] Celestial
[5] Complexity
[6] Dynomics
[7] Complex Adaptive Systems

کاهش داده و قادر به ارائه پاسخ‌های مناسب با هر یک از وضعیت‌های پیچیده مبتنی بر تحلیل رابطه علت و معلول باشد. چارچوب کانوین، شرایط گوناگون محیطی را براساس نوع رابطه علت و معلول به دامنه‌ها[8] یا وضعیت‌های پنج‌گانه تقسیم‌بندی کرده و متناسب با اینکه در چه وضعیتی هستیم به ارائه راهکار و روش مواجهه می‌پردازد. مدیریت امنیت فضای سایبر نیز تحت سیستم‌های پیچیده انطباقی قابل بررسی است که مدل کانوین به خوبی جهت مواجهه با آن برای تصمیم‌گیری با هدف کاهش ریسک قابل بهره‌گیری می باشد.

در ادامه به طور مختصر در خصوص امنیت فضای سایبر، پویایی و پیچیدگی‌های آن و متعاقباً ضرورت بکارگیری مدلی مانند کانوین برای تصمیم‌گیری فراخور وضعیت‌های گوناگون در آن اشاره خواهیم کرد. سپس ضمن معرفی کوتاه چارچوب کانوین به طرح یک سناریوی امنیتی در فضای سایبر پرداخته و در ادامه با بکارگیری چارچوب کانوین برای هر یک از وضعیت‌های رخ داده حاصل از اقدام ضد امنیتی سایبر مطابق با سناریوی مطروحه، روش مواجهه را ترسیم نموده و در پایان نتیجه‌گیری خواهیم داشت.

۲. چارچوب کانوین در مواجهه با مسائل امنیتی فضای سایبر

در این بخش ابتدا به ماهیت پیچیدگی و پویایی امنیت در فضای سایبر پرداخته و ضمن معرفی چارچوب کانوین به شرح نحوه بکارگیری آن جهت کمک به تصمیم‌گیری با هدف کاهش ریسک و حل مسائل امنیتی در فضای سایبر با ارائه یک سناریوی فرضی خواهیم پرداخت.

۲-۱. پویایی و پیچیدگی امنیت فضای سایبر

می توان گفت اکثر کارهای مرتبط با آگاهی وضعیتی در حوزه سایبر بر روی تکنولوژی برای جمع آوری، تجزیه و تحلیل و کشف همبستگی داده‌ها متمرکز بوده است. به نظر می‌رسد که این اطلاعات به انسان‌ها برای تصمیم‌گیری بهتر، کمک می‌کنند. اما برخلاف روش‌های تکنولوژی محور در تصمیم‌گیری‌های فضای سایبر، روش‌های انسانی به ندرت بکار گرفته شده‌اند(Durso, Sethumadhavan, 2008). به تازگی یکی از انجمن‌ها که تحقیقی به نام "آگاهی وضعیتی سایبری شناختی" را به عنوان یک مثال منتشر نموده، وارد این عرصه شده است. در این تحقیق از مفاهیم فیوژن داده برای جلوگیری از سردرگمی و بهبود آگاهی وضعیتی انسان محور بهره برده‌اند(Gutzwiller, et al., 2016).

در شرایط بحرانی مانند حملات سایبری بلادرنگ و یا نقض داده‌ها، تصمیم‌گیری‌های انسانی بسیار مهم می‌شود. چرا که عملیات سایبری امروز بسیار پویاست(Josiah, et al., 2016).

اکثر اقدامات سایبری تحلیلگران و مدافعانی دارد که ضمن آمادگی همیشگی باید قدرت واکنش و پاسخگویی به دشمنان را داشته باشند، چرا که اقدامات دشمنان می‌تواند بطور مداوم تغییر و غیرقابل پیش‌بینی باشد. وضعیت‌های نامعلوم، پیچیده و پویا همانند وضعیت‌های مربوط به امنیت سایبر محیط پرریسکی را ایجاد می‌نمایند. وضعیت های پویا مستلزم بکارگیری روش‌های تصمیم‌گیری پویا است و اغلب تصمیم‌گیرندگان جز تعداد محدود، متکی به رویکردهای مشترکی هستند که به خوبی در یک مجموعه از شرایط خاص کار می‌کنند.

وضعیت محیطی، یک عنصر مهم تصمیم‌گیری می‌باشد. مدل‌های فکری نادرست می تواند ناخودآگاه تصمیمات را دچار گمراهی کند، اما خودآگاهی سنجیده شده می تواند تصمیم‌گیری را بهبود بخشد(Mugan, 2014).

امنیت سایبری با ماهیت دفاعی خود، اساساً در مواجهه با وضعیت‌های ناشناخته[9] است چرا که مدافعین امنیت سایبری همیشه باید استنتاج کنند یا استدلال کنند که دشمنان چه فکری می‌کنند، چه برنامه‌ریزی دارند و چه اقدامی انجام می‌دهند، که همگی در هاله‌ای از ابهام و ناشناختگی قرار دارد.

8

9 Unknown

عموماً تکنولوژی و مهندسی برای حل مشکلات دارای نظم[10]، ساختاریافته و قابل اندازه‌گیری در جوامع، مناسب می‌باشند حال آن که امنیت سایبری دارای محیط پیچیده است که همیشه با مهندسی قابل حل نیست(Gutzwiller, et al., 2016).

از طرفی آینده جنگ‌های سایبری بی‌دریغ با مشارکت هکتویست‌ها[11] (هکرهایی که فعالیتشای در راستای تبلیغ و یا خودنمایی علمی یا اختلافات اجتماعی یا سیاسی است و درصدد ارسال پیام‌های سیاسی یا اجتماعی یا ایدئولوژیک خود از طریق فضای سایبر به سراسر جهان می‌باشند) خواهد بود، و در این حالت درک ساختار اخلاقی آن‌ها زمینه را برای تصمیم‌گیری علیه اقدامات مخرب آن‌ها در تمام سطوح جنگ فراهم می‌سازد(Mugan, 2014).

درک ساختار اخلاق هکتویست‌ها، از طریق شناسایی وضعیت‌هایی از فضای سایبر که ناشی از حضور آن‌هاست به ما کمک می‌کند تا بتوانیم تصمیمات صحیحی را برای مواجهه به هر یک از موقعیت‌های محیطی و زمان‌های متفاوت حاصل از اقدامات آن‌ها اتخاذ کنیم. قابل توجه است که وضعیت‌های حاصل از فعالیت‌ها، هکتویست‌ها در فضای سایبر نیز از طریق کشف «چگونگی انجام فعالیت‌های آن‌ها» در مکان‌ها و زمان‌های گوناگون در فضای سایبر امکان‌پذیر است. بدیهی است شبکه‌های اجتماعی بستر مناسبی برای ظهر و بروز اینگونه اقدامات خواهد بود.

نتیجه اینکه چارچوب‌های اخلاقی و مهندسی فعلی در مواجهه با مسائل امنیت سایبری در حال حاضر و یا ساختار اخلاق هکتویست‌ها در آینده برای دسته بندی رفتارها، فعالیت‌ها و علت های هر یک از مخربین امنیتی کافی نخواهد بود و لذا نیازمند چارچوب و رویکرد دیگری در مواجهه با مسائل امنیت فضای سایبر برای تصمیم‌گیری صحیح و کاهش ریسک در این فضا خواهیم بود.

اسنودن[12] و بون[13]، به عنوان معماران چارچوب کانوین می گویند، درک عمیق از وضعیت و یا زمینه محیطی توانایی پذیرش پیچیدگی، تناقض‌ها همراه با کمی انعطاف‌پذیری، شیوه‌های رهبری رهبرانی که می‌خواهند در شرایط عدم قطعیت تصمیماتی را اتخاذ کنند و اتفاقاتی را رقم بزنند را تغییر می دهد. در واقع این فرآیند تبدیل وضعیت ناشناخته[14] به وضعیت شناخت‌شده[15] ما را قادر می‌سازد تا درست درک کنیم، فهم کنیم، اثرات یا اتفاقات را به عوامل یا علل آن ها نسبت دهیم، قیاس نماییم و نهایتاً پیش‌بینی کنیم(Snowden, Boone, 2007).

در این پژوهش یک رویکرد متفاوت بر تصمیم‌گیری در مورد مسائل امنیت سایبری پیشنهاد می‌کنیم، که نشان می دهد چگونه سیگنال‌های ضعیف ناشی از ریسک‌های در حال ظهور در مراکز عملیات امنیت سایبری شناسایی و تفسیر شده و همین طور چگونه از آن‌ها در چارچوب کانوین برای تصمیم‌گیری پویا جهت درک و مدیریت ریسک بهره خواهیم برد.

۲-۲. چارچوب کانوین

معنابخشی[16] یک روش و فرآیند برای سازماندهی مسائل ناشناخته و مجهول و همچنین به عنوان بخشی از فرآیند آگاهی وضعیتی است(Durso, Sethumadhavan, 2008).

این فرآیند با یک ادراک احتمالی یا تصویری از دنیای پویا و در حال تغییر آغاز شده، با مقایسه این تصویر با سایر تصاویر از طریق جمع‌آوری داده‌ها ادامه یافته و سپس با اقدام، تعامل با محیط و در نهایت پالایش یا عبور از وضعیت تصویر فعلی از دنیای ترسیم شده بسته به اینکه این تصویر دارای اعتبار هست یا خیر، خاتمه می‌یابد(Ancona, et al., 2011).

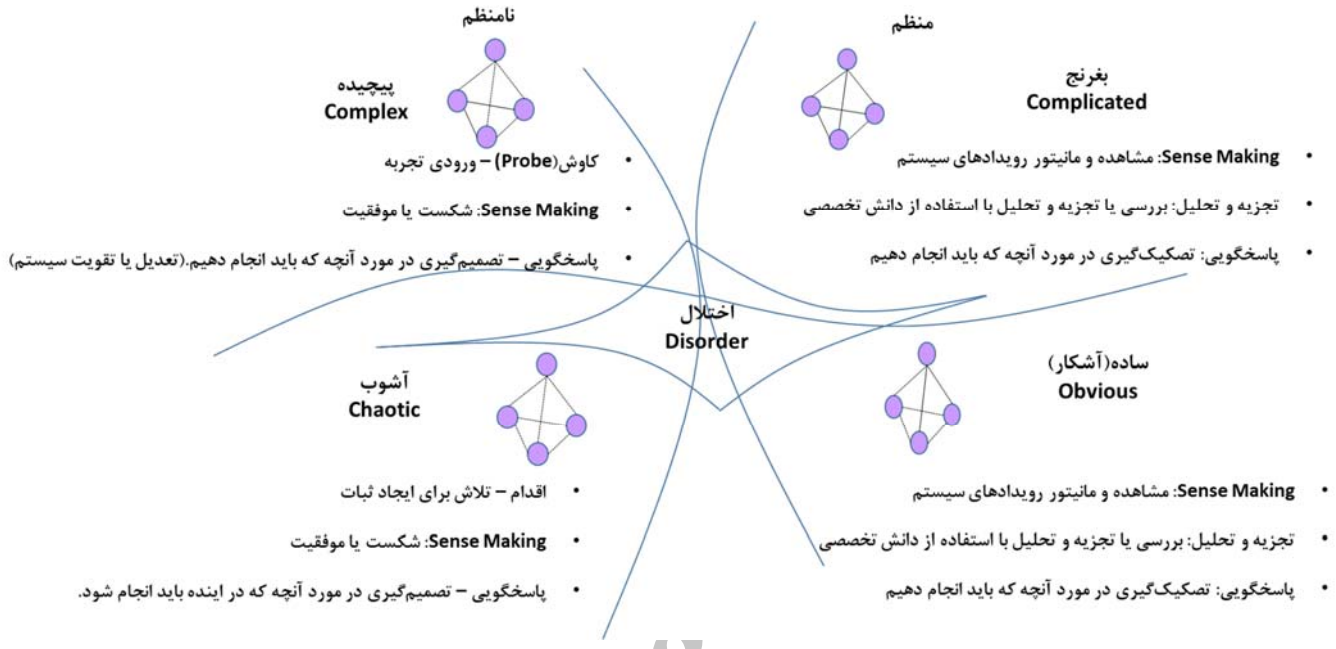
این روش در زمان‌هایی که درک کمی از محیط کار داریم و زمانیکه تصمیم‌گیری‌ها باید سریع انجام شود مناسب است. معنابخشی یک رویکرد برای کشف کاری است که باید در شرایط محیطی متفاوت انجام دهیم.

---

[10] Ordered
[11] Hacktivist
[12] Snowden
[13] Boone
[14] Unknown
[15] Known
[16] Sense-making

چارچوب کانوین یک ابزار معنابخشی است که توسط دیو اسنودن ساخته شده و اولین بار در سال ۱۹۹۹ به‌کار گرفته شده است(Snowden, 1999).

این چارچوب که در تصویر شماره ۱ نشان داده شده است، شامل پنج دامنه است که مشکلات و یا موقعیت‌ها را توصیف می‌کنند و نوع اقدام را متناسب با این دامنه‌ها(اختلال، آشکار، بغرنج، پیچیده و آشوب) مشخص می‌کند.



- **دامنه اختلال[17] در کانوین**

حالتی است که هیچگونه شناختی از رابطه بین علت و معلول نسبت به مسئله یا وضعیت خاص وجود نداد. در این حالت، افراد خود را نسبت به تصمیم‌گیری آزاد می‌دانند. هنگامی که شما نمی‌دانید در چه دامنه **دیگری قرار دارید در واقع، اختلال یک وضعیت پیش**فرض است.

- **دامنه آشکار[18] یا ساده در کانوین**

در دامنه آشکار(ساده) رابطه بین علت و معلول به وضوح قابل درک است. حقایق وضعیت ارزیابی، طبقه‌بندی و سپس بر اساس بهترین اقدام یا عمل یک پاسخ اجرا می‌شود. این دامنه دارای ریسک بسیار کمی است چراکه کمترین ناشناختگی یا ابهام نسبت به وضعیت وجود دارد. در دامنه آشکار رویکرد "بهترین شیوه" عمل می‌کند. در حالیکه شرایط از موردی با موارد دیگر متفاوت است. شیوه‌های از قبل ایجاد شده برای واکنش و پاسخ به تهدیدات و همچنین درک صحیحی از نتایج اقدام وجود دارد.

[17] Disorder Domain
[18] Obvious or Simple Domain

- **دامنه بغرنج[19] در کانوین**

در این دامنه، رابطه بین علت و اثر لزوماً به خوبی درک نشده و نیاز به کمک گرفتن از تجزیه و تحلیل متخصصان و خبرگان مرتبط با موضوع می‌باشد. گزینه‌های مختلف باید مورد بررسی قرار گیرد، توصیه‌های متخصصان باید در نظر گرفته شده و سپس بر اساس تجزیه و تحلیل صورت گرفته، اقدام شود.

- **دامنه پیچیده[20] در کانوین**

در دامنه پیچیده، رابطه بین علت و اثر را نمی‌توان بلافاصله درک کرد، و اغلب با نگاه به گذشته می‌توان رابطه‌ای بین علت و معلول یافت. ایده‌های مختلفی برای بررسی اینکه آیا آن‌ها به وضعیت کمک می‌کنند یا خیر آزمایش می‌شوند. اگر این ایده‌ها کمک کننده باشند، تقویت می‌شوند و اگر نه، آن‌ها تضعیف می‌شوند و ایده‌های دیگری آزمایش می‌شوند.

- **دامنه آشوب[21] در کانوین**

در دامنه آشوب(هرج و مرج) بین علت و معلول رابطه‌ی قابل توجهی وجود ندارد. تصمیم‌گیری‌های فوری ویژه‌ای برای تثبیت در اولویت هستند، گام بعدی تلاش برای درک و یافتن ریشه و علل هرج و مرج است. در دامنه آشوب اقدام جدید، ایده خوبی است.

۲-۳. سناریوی فرضی در امنیت فضای سایبر

شبکه‌های اجتماعی یک بستر ارتباطی است که امکان ملاقات، ارسال نظرات، نشر و دریافت انواع محتوای دیجیتال و امروزه انجام تراکنش‌های مالی و حتی راه‌اندازی کسب و کارها را برای افراد فراهم آمده است. در کنار تمام مزایای موجود، تعداد زیادی از افراد هستند که از وب سایت‌های شبکه‌های اجتماعی به عنوان راهی برای سرقت اطلاعات شخصی، به ویژه از طریق فیشینگ، و همچنین سودجویی مالی از طریق انتشار باج‌افزارها استفاده می‌برند.

اغلب کاربران شبکه‌های اجتماعی موارد امنیتی به ویژه تنظیمات حریم خصوصی را بر روی حساب‌های شخصی خود در رسانه‌های اجتماعی که عضو هستند رعایت نمی‌کنند و در سطح پایینی از امنیت به فعالیت خود ادامه می‌دهند. لذا این فضا را برای یادگیری و کشف اطلاعات حیاتی شخصی توسط مجرمان سایبری مستعد می‌سازند. اطلاعاتی از قبیل محل و تاریخ تولد، سلایق شخصی کاربران از طریق تایید[22] یا عدم تایید[23]، تیم‌های ورزشی مورد علاقه نمایش‌ها، تلویزیون و حتی اطلاعات مالی تنها تعدادی از اطلاعاتی است که کاربران در معرض سوء استفاده قرار می‌دهند. و مجرمان سایبری با فهم درست از این اطلاعات و تحلیل اندک، به‌واسطه حملات فیشینگ[24] به انتشار محتوایی که احتمالاً منضم به بدافزارها و باج‌افزارهاست، به مقصد خواهند رسید. سازمانی را در نظر بگیرید که کسب و کار آن براساس یکی از شبکه‌های اجتماعی شکل گرفته است. این سازمان دارای یک شبکه داخلی می‌باشد که کارکنان ضمن بهره‌گیری از رایانه‌های اداری جهت به اشتراک‌گذاری منابع، امکان اتصال به اینترنت جهت وظایف محوله در راستای کسب و کار شرکت نیز می‌باشند. هر یک از کارکنان با عضویت در شبکه اجتماعی منتخب سازمان از طریق حساب‌های کاربری، ضمن انجام امور محوله در راستای کسب و کار سازمان که مبتنی بر بازاریابی مدل شبکه‌ای است، به انجام امور شخصی خود اعم از ارسال و دریافت انواع محتوای دیجیتال و یا حتی برخی تراکنش‌های مالی نیز می‌پردازند. در نتیجه بخش اعظمی از اطلاعات شخصی هر یک از آن‌ها خواسته یا ناخواسته در معرض تهدید مجرمان سایبری قرار دارد که می‌تواند مورد سوء استفاده قرار گیرد.

---

[19] Complicated Domain
[20] Complex Domain
[21] Chaotic Domain
[22] Likes
[23] Dislikes
[24] Phishing

باید در نظر داشت رایانه‌ای که در اختیار هر یک از کارکنان قرار دارد ضمن انجام فعالیت‌های مربوط به کسب و کار سازمان، حاوی اطلاعات مهم سازمانی و شخصی به دلیل انجام فعالیت‌های موردی می‌باشد.
سناریو از این قرار است که کارکنان دپارتمان فناوری اطلاعات سازمان مذکور از تعدادی تلاش‌های مبتنی بر حملات فیشینگ در روز مطلع می‌شوند. ساعات آغازین یکی از روزهای کاری تعداد زیادی از کاربران سازمان طی تماس تلفنی اذعان می‌دارند که دسترسی آن‌ها به شبکه و یا رایانه‌های شخصی قطع شده است. بررسی دقیق‌تر اولیه نشان می‌دهد که یک باج افزار در سراسر شبکه گسترش یافته است و حساب‌های کاربری برای دسترسی به رایانه‌های شخصی را قفل و اطلاعات برخی از رایانه‌ها را نیز رمزگذاری می‌کند تا زمانی که هزینه‌ای پرداخت شود.

۲-۴. تصمیم‌گیری براساس چارچوب کانوین در مواجهه با سناریوی امنیت سایبری

با عنایت به سناریوی مطروحه در بخش قبلی، در این قسمت نگاشتی از هر یک از وضعیت‌های محتمل ناشی از حمله سایبری به دامنه‌های پنج‌گانه مدل کانوین داشته و سپس راهکار مواجهه با شرایط مترتب بر وضعیت موجود را براساس توصیه‌های چارچوب کانوین متناسب با دامنه‌های که در آن هستیم برای کمک به تصمیم‌گیری در جهت مدیریت محیط و کاهش ریسک و بهبود شرایط ارائه می‌دهیم.

۲-۴-۱. تصمیم‌گیری در وضعیت بی نظمی یا اختلال[۲۵] (Disordor) حاصل از سناریوی امنیت سایبری

در خصوص سناریوی مذکور، هنگامی که تیم فناوری سازمان برای اولین بار تماس‌هایی دریافت می‌کنند مبنی بر اینکه که کاربران نمی‌توانند به شبکه دسترسی داشته باشند، سازمان در دامنه بی‌نظمی یا اختلال به سر می‌برد، زیرا آن‌ها علت این موضوع را اصلاً نمی‌دانند. در این حالت براساس الگوی کانوین، این تیم باید به شکل محسوس با جمع‌آوری اطلاعات در خصوص شرایط و واقعه، سعی نماید خود را در یکی از وضعیت‌های ۴ گانه دیگر چارچوب کانوین احصاء کند تا امکان اقدامی را فراهم کرده باشد (Gutzwiller, et al., 2016). در این سناریو جمع آوری اطلاعات حاکی از آلودگی بخش عمده‌ای از اطلاعات اشخاص در رایانه‌ها و حساب‌های کاربری می‌باشد که توسط باج‌افزار صورت گرفته است.

۲-۴-۲. تصمیم‌گیری در وضعیت آشکار یا ساده[۲۶] حاصل از سناریوی امنیت سایبری

هنگامی که کارکنان فناوری اطلاعات سازمان با اطلاعات جمع‌آوری شده در می‌یابند که باج‌افزار علت قطعی شبکه بوده و علت و معلول تأخیر و قطعی شبکه مشخص می‌شود. در این وضعیت در یک دامنه کاملاً آشکار قرار داریم و گزینه‌های فوری متعددی جهت پاسخگویی و اقدام وجود دارد. این سازمان باید بهترین شیوه پاسخ دادن به وضعیت فعلی را از میان گزینه‌های آماده شناسایی و مناسب‌ترین را اجرا کند. بطور مثال در راهکارهای از قبل‌آماده خود به توصیه سمانتک مبنی بر حذف سیستم‌های آلوده از شبکه و بررسی جهت چگونگی بازیابی فایل‌های آسیب دیده از روی پشتیبان‌های فایل‌ها برمی‌خورد و این گزینه را بهترین راهکار و در نهایت عملی می‌کند(Sherman, 2015).

[25] Disorder Domain
[26] Obvious or simple

۲-۴-۳. تصمیم‌گیری در وضعیت بغرنج[۲۷] یا درهم‌تنیده حاصل از سناریوی امنیت سایبری

پس از آنکه کارکنان بیمارستان بهترین شیوه برای تثبیت شبکه را اجرا کرده‌اند، ممکن است خود را در معرض چندین گزینه مواجه بدانند به عنوان مثال در این حالت آن‌ها نمی‌دانند که علت حمله می‌تواند فیشینگ، بهره‌برداری از راه دور[۲۸] یک سرور اینترنتی، یک مهاجم داخلی[۲۹] و یا دیگر منابع باشد. در این حالت در وضعیت بغرنج به سر می‌برند که ضروری است به دنبال متخصصان و تحلیلگران خبره مرتبط با موضوع یعنی جرم‌یابی قانونی دیجیتال[۳۰] یا امنیت سایبری برای کمک به ارزیابی وضعیت موجود و ارائه توصیه‌های لازم برای گام‌های بعدی باشند.

۲-۴-۴. تصمیم‌گیری در وضعیت پیچیده[۳۱] حاصل از سناریوی امنیت سایبری

در سناریوی امنیتی مطروحه، نتایج تجزیه و تحلیل قانونی و تکرار آن در نهایت ممکن است نشان دهد که یکی از کارمندان به اشتباه و بطور سهوی ضمیمه یک ایمیل مخرب را که در واقع نوعی حمله فیشینگ بود، باز کرده است. حملات سمت مشتری[۳۲] می تواند یک وضعیت پیچیده را به وجود آورد چرا که در این حالت تنها پس از آن‌که کارشناسان خبره علت حمله را تشخیص دادند، مقابله احتمالی را نیز انجام دادند، دانش و روش لازم دفاع بدست می‌آید. در چنین وضعیتی دانش و روش لازم دفاع اشاره به فعالیت سازمان مبنی بر مسدودسازی ایمیل‌های خرابکارانه و نرم افزارهای مخرب با استفاده از اکتشاف و آزمایشات مکرر دارد. در دامنه پیچیده، اقدامات تابع پدیده‌ها، نوظهور و ناگهانی می‌باشند.

۲-۴-۵. تصمیم‌گیری در وضعیت آشوب[۳۳] حاصل از سناریوی امنیت سایبری

در سناریوی مطروحه، نباید خود را در دامنه آشوب ببینید، اما تغییرات احتمالی، ممکن بود که شما را اول وادار به اقدام و سپس درک علت کند. اگر اولین نشانه حمله گواه انتشار اطلاعات شخصی و یا سلامتی افراد که ناشی از نقض داده‌هاست بود، و نشانه دوم پیدا کردن فیشینگ و باج‌افزار به عنوان دلیل واقعه بود، آنگاه در وضعیت آشوب قرار گرفته‌اید که چارچوب کانوین توصیه می‌کند در چنین شرایطی ابتدا اقدامی را برای ثبات در وضعیت انجام داده و سپس به دنبال کشف علت بگردید. به‌طور مثال در واقعه نقض داده‌های کمپانی Home Dept انتشار مطبوعاتی در مورد کنترل خسارات قبل از گزارش‌های مربوط به تحلیل رویداد منتشر شده است.

---

[27] Complicated Domain
[28] Remote Exploitation
[29] Insider Attacker
[30] Digital Forensics
[31] Complex Domain
[32] Client – Side Attack
[33] Data Breach

۳. نتیجه‌گیری

الزاماً در تمامی محیط‌ها به ویژه محیط‌هایی که در آن مسائل بر اساس رابطه بین علت و معلول قابل دسته‌بندی بوده و به تناسب نوع رابطه قابل تعمیم به وضعیت‌های گوناگون می‌باشند مواجهه سیستمی پاسخگو نبوده و لذا نیازمند نوعی نگاه جدید و متفاوت برای حل مسائل می‌باشیم. در این پژوهش محققان نشان داده‌اند که تصمیم‌گیری در محیط‌های پیچیده یک اقدام دارای ریسک می‌باشند. کانوین یک مدل مناسب برای بکارگیری در انواع اکوسیستم‌های پیچیده از قبیل پزشکی، خطرات زنجیره غذایی، هوانوردی، اخلاق نظامی و امنیت می‌باشد.

ما با ترسیم یک سناریوی فرضی در حوزه امنیت سایبری، تلاش نمودیم تا نگاشت صحیحی در بکارگیری چارچوب کانوین نسبت به فضای مسئله ایجاد نموده و با بهره‌گیری از این چارچوب به تصمیم‌گیرندگان امکان تشخیص وضعیت‌های مرتبط با رویداد سایبری را داده و راه‌حل‌های نوآورانه را در شرایط پیچیده برای مواجهه با محیط و حل مشکل ارائه دادیم.

مراجع

Ancona, D., Snook, N. N., & Khurana, R. (2011). *Sensemaking: Framing and acting in the unknown* in Handbook of Leadership Education, Los Angeles:SAGE, pp. 3-19.

Durso, F. T., & Sethumadhavan, A. (2008). *Situation awareness:Understanding dynamic environments, Human Factors*, vol. 50, no. 3, pp. 442–448.

Dykstra, A. B. S., & Orr, R., IV. (2016). *Acting in the unknown: the cynefin framework for managing cybersecurity risk in dynamic decision making*, IEEE International Conference on Cyber Conflict (CyCon U.S.), Washington, DC, USA, 21-23 Oct.

Gandhi, G. (2014, May). *Complexity Theory in Cyber Security.* The University of Warwick.

Gutzwiller, R. S., Hunt, S. M., & Lange, D. S. (2016). *A task analysis toward characterizing cyber cognitive situational awareness (CCSA)*, IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support.

McLeod, S. A. (2008). *Reductionism and holism*,Retrieved from https://www.simplypsychology.org/reductionism-holism.html

Mugan, J. (2014). *The Curiosity Cycle*, Buda, TX:Mugan Publishing.

Scott, W., & Shawn Cupp, O. (2017). *Ethics of Hacktivism*. 2017 Fort Leavenworth Ethics Symposium, April 24-25.

Sherman, M. (2015). *Ransomware Do's and Don'ts: Protecting Critical Data.* Available from: https://www.symantec.com/connect/blogs/ransomware-dos-and-donts-protecting-critical-data.

Snowden, D. J. (1999). *The paradox of story: Simplicity and complexity in strategy*, Scenario and Strategy Planning, vol. 1, no. 5, pp. 16-20.

Snowden, D. J., & Boone, M. E. (2007). *A leader's framework for decision making*, Harvard Business Review, pp. 69-76, November.

The use of the Cynefin framework in the face of the dynamics and complexity of cyberspace security

Mohammad Abedi
Faculty of National Security, National Defense University of Iran, Tehran, Iran, E-mail: m.abedi@sndu.ac.ir

Mohammad Reza Karimi Ghohroodi
Malek-Ashtar University of Technology, Tehran, Iran,
E-mail: favad110@gmail.com

Abstract. Deciding in complex and dynamic environments such as cyberspace, which is associated with rapid changes and diversity have high risk .Unfortunately, most research on cyber state awareness has focused on technology and has not paid much attention to human-based decisions. While in critical situations, such as real-time attacks, there is a need for human intervention in decision making. For this reason, cyber security professionals and managers need a model or framework for making decisions that are appropriate to any situation caused by cyber security crises. In this research, we will introduce the Cynefin framework and how it will be used to make the right decision in dealing with the various situations caused by a cyber-attack to reduce risk. In addition to mapping the situations of cyberattack in the hypothetical scenario on the five domains of the Cynefin framework, such as disorder, obvious, complicated, complex, and chaotic, we will eventually show how the Cynefin framework can help professionals and managers recognize the current state of affairs and the appropriate response in complex conditions, based on the relationship of cause and effect.

Keywords: Cynefin framework, Cyberspace Security, Complexity, Complex Adaptive Systems, Decision making