نشریه علمی "پدافند الکترونیکی و سایبری"
سال هفتم، شماره ۴، زمستان ۱۳۹۸، ص ۱۱۵-۱۰۵

ارائه یک روش بهبودیافته تشخیص رخداد ناشی از حملات سایبری

محمدحسین حسن‌نیا[۱]، محمدرضا حسنی‌آهنگر[۲*]، آرش غفوری[۳]
۱- کارشناس ارشد امنیت اطلاعات، ۲- دانشیار، ۳- پژوهشگر، دانشگاه جامع امام حسین(ع)

(دریافت: ۹۷/۰۹/۱۳، پذیرش: ۹۸/۰۳/۲۸)

چکیده

خطای نیروی انسانی در طراحی و پیکربندی شبکه‌ها و سامانه‌ها، بستری برای حمله است و از طرفی شبکه‌های گسترده ازنظر جغرافیایی در معرض حملات بیشتری بوده و نیاز به شناسایی زودهنگام حملات دارند. مرکز عملیات امنیت سایبری که معمولاً در شبکه‌های گسترده استفاده می‌شود، راه‌کاری برای پایش و شناسایی پیوسته است و در آن، نیروی انسانی نقش اصلی را ایفا می‌کند. در این تحقیق با بررسی موضوع مصورسازی و مقایسه نمونه‌های تجاری مراکز عملیات امنیت، روشی برای کمک به تشخیص بی‌درنگ حملات در شبکه‌های گسترده ارائه شده است. روش پیشنهادی مصورساز پدافند سایبری (مُپسا) این است که یک مؤلفه مصورساز بی‌درنگ حملات سایبری در سامانه مرکز عملیات امنیت اضافه شود تا تحلیل‌گرها با استفاده از داده‌های آن و دیگر داده‌ها، بتوانند به‌صورت زودهنگام، در مورد تغییرات لازم در شبکه‌ها، تصمیم‌گیری کنند. این راه‌کار باعث کاهش خطای نیروی انسانی، افزایش کارایی آن و افزایش سرعت اعمال تغییرات می‌شود و بنابراین، اثر حملات به شبکه‌های گسترده را کاهش می‌دهد.

کلید واژه‌ها: مرکز عملیات امنیت، مصورسازی، بی‌درنگ، حملات سایبری

۱. مقدمه

در طی چند سال اخیر مهم‌ترین مخاطره سایبری، ظهور حملات توزیع‌شده سایبری و همه‌گیری توقف‌ناپذیر آن در دنیاست. این نوع حملات با سوءاستفاده از بستر فراهم‌شده در دهکده جهانی اینترنت، منابع مالی، نظامی و به‌طور کل راهبردهای دولت‌ها و جوامع را مورد هدف قرار داده است. حملات توزیع‌شده تهدیدات متعددی را موجب می‌شود که مهم‌ترین آن‌ها *DDoS*، *Phishing*، *Fast-fluxing* و *Data Theft* می‌توانند خطرآفرین باشند [۵-۱].

سامانه‌های موجود در شبکه‌های گسترده ازنظر جغرافیایی به دلیل گستردگی این شبکه‌ها، تحت حملات سایبری گسترده‌تری قرار می‌گیرند که می‌تواند موجب نشت اطلاعات در این شبکه‌ها شود. لذا حفاظت از داده‌ها در شبکه‌های گسترده، نیاز به تلاش و نظارت سریع‌تر و دقیق‌تر دارد.

با توجه به محبوبیت استفاده از تجهیزات مختلف ارتباطی از قبیل کامپیوترهای همراه، تلفن همراه، گوشی‌های هوشمند برای اتصال به شبکه و همچنین افزایش رخدادهای سایبری اخیر در دنیا مانند حملات روز صفر[۱]، حملات توزیع‌شده، تهدیدات پیشرفته پایدار[۲]، ارائه راه‌کارها و روش‌های امن ضروری است.

بنابراین، محققان امنیت سایبری با توجه به سرعت حملات سایبری، تحقیق و توسعه را نیز بر روی خودکارسازی روند تشخیص و پاسخ حملات متمرکز کرده‌اند [۶].

در حوزه امنیت شبکه‌های رایانه‌ای، برای بهبود وضعیت امنیتی و همچنین رصد و پایش و مقابله با تهدیدات سایبری پیشنهاد می‌شود برای آموزش کارمندان، همگون کردن نرم‌افزارها و سخت‌افزارها، ثبت دارائی‌ها، یکپارچگی ثبت فعالیت‌ها و همچنین بصری‌سازی رویدادهای امنیتی برنامه‌ریزی‌های لازم در سازمان صورت گیرد.

از طرفی انسان که ضعیف‌ترین حلقه زنجیره امنیت است و اگر فرهنگ‌سازی و آموزش لازم و کافی در زمینه امنیت صورت نگیرد تمام تمهیدات فنی و کارشناسی تأثیر خود را از دست خواهند داد. بنابراین، باید راه‌کارهایی برای افزایش سرعت عملکرد و کاهش خطای نیروی انسانی اندیشیده شود. البته این نکته قابل توجه است که از طریق رایانه‌ها می‌توان موارد بسیاری را پیگیری و دنبال کنند، اما انسان‌ها همچنان قادر به درک، منطق و پیش‌بینی سطح بالاتری هستند لذا راهبران امنیت سایبری خواستار تجسم‌هایی هستند که می‌تواند عملکرد انسان را در عملیات‌های امنیت سایبری تقویت کند [۷].

مزایای مصورسازی شامل پاسخ به پرسش‌ها، ایجاد پرسش‌های جدید، کاوش و اکتشاف، کمک به تصمیم‌گیری،

*رایانامه نویسنده مسئول: mrhasani@ihu.ac.ir

[1] Zero-day
[2] Advanced Persistent Threats (APT)

انتقال اطلاعات، افزایش کارایی و الهام بخشی است. بنابراین، روش مصورساز پدافند سایبری برای مؤلفه نیروی انسانی در مرکز عملیات امنیت، این مزایا را به همراه دارد.

کارشناسان امنیتی نه تنها حملات سایبری را با استفاده از مصورسازی تحقیق می‌کنند، بلکه به‌صورت بصری نیز می‌بینند [۸]. لذا بصری‌سازی رویدادهای امنیتی یکی از موارد بسیار مهمی است که به مدیران و کارشناسان کمک می‌کند تا بتوانند در مقابله با تهدیدات سایبری برنامه‌ریزی لازم را انجام دهند. چراکه این مؤلفه می‌تواند اثربخشی مناسبی در حوزه امنیت و پدافند سایبری داشته باشد بدین‌صورت که با مصورسازی بی‌درنگ حملات سایبری و نمایش آن به راهبران سامانه، باعث افزایش سرعت تصمیم‌گیری و برنامه‌ریزی برای سامانه‌ها و شبکه‌های رایانه‌ای می‌شود و خطاهای ناشی از پیکربندی‌های اشتباه را کاهش می‌دهد.

بنابراین، روش پیشنهادی در این تحقیق این است که در مرکز عملیات امنیت که مرکز پایش و مقابله با تهدیدات سایبری است، از مصورساز بی‌درنگ حملات سایبری استفاده شود تا حملات صورت گرفته علیه شبکه‌های گسترده به‌سرعت تشخیص داده‌شده و تصمیم‌گیری‌ها و برنامه‌ریزی‌های لازم به‌سرعت انجام شود.

مصورساز پدافند سایبری، این امکان را می‌دهد که درآن‌واحد و به‌صورت بی‌درنگ حملات سایبری که در سراسر شبکه انجام می‌شود را روی یک نقشه به‌صورت بی‌درنگ مشاهده کرد. این نقشه، شدت حملات در مکان‌های جغرافیایی را برحسب رنگ‌های مختلف نشان می‌دهد تا تحلیل‌گران متوجه شوند که در هرلحظه کدام‌یک از نقاط شبکه بیشتر مورد حملات سایبری قرار می‌گیرند.

مقاله حاضر شامل شش بخش است. در بخش دوم ادبیات موضوع موردبحث قرار می‌گیرد. در بخش سوم چند سامانه مرکز عملیات امنیت موردبحث قرار می‌گیرد و سپس محصولات تجاری موردبررسی و مقایسه قرار خواهد گرفت. در بخش چهارم روش پیشنهادی تشریح خواهد شد. در بخش پنجم روش پیشنهادی با شبیه‌سازی حملات مورد ارزیابی قرار می‌گیرد و درنهایت در بخش ششم جمع‌بندی این مقاله ارائه می‌گردد.

۲. مفاهیم پایه

در این بخش مفاهیم و مبانی نظری و کاربردی مربوط به حملات سایبری توزیع‌شده از قبیل مصورسازی حملات سایبری و مرکز عملیات امنیت موردبحث و بررسی قرار می‌گیرد.

۲-۱. مصورسازی

همان‌طوری که یک تصویر بهتر از هزار کلمه است. در دنیای امنیت هم یک تصویر، از هزار رویداد ثبت‌شده بهتر است. به‌جای اینکه فردی یک فایل ثبت رویداد را که شرح وقوع یک حمله را ثبت کرده است، بررسی کند، می‌تواند از یک تصویر استفاده نماید که بازنمایی مصوری از رویدادهای ثبت‌شده است. تصویر با یک نگاه، محتوای ثبت رویداد را انتقال می‌دهد. مصورسازی در بحث امنیت به معنی فرایند تولید تصویر بر مبنای رویدادهای ثبت‌شده است. مصورسازی در اینجا چگونگی نگاشت رویدادهای ثبت‌شده به یک تصویر را تعریف می‌کند [۹].

راه‌های تحلیل داده‌های امنیت با استفاده از رویکرد مصور را می‌توان به سه دسته تقسیم کرد [۹]:

۱. گزارش‌گیری[1]
۲. تحلیل‌های مربوط به گذشته[2]
۳. نظارت بی‌درنگ[3]

تمرکز نظارت بی‌درنگ بر آگاهی از وضعیت فعلی سامانه‌ها، شبکه‌ها و برنامه‌های کاربردی و همچنین فعالیت‌ها و رویدادهایی است که در حال حاضر انجام می‌شوند. واضح است که این‌رویدادها به‌طور مستقیم بر وضعیت فعلی تأثیر گذاشته و درنتیجه آن را تغییر می‌دهند. برای نمایش وضعیت رویدادهای فعلی، از داشبوردها استفاده می‌شود [۹]. استفان فیو، در کتاب خود درباره طراحی داشبوردهای اطلاعات [۱۰]، داشبورد را این‌گونه تعریف می‌کند:

" داشبورد، ارائه گرافیکی مهم‌ترین اطلاعات مورد نیاز برای رسیدن به یک یا چند هدف مشخص است که در یک صفحه با دقت و نظم چیده شده‌اند تا در یک نگاه قابل نظارت باشند."

۲-۲. مرکز عملیات امنیت

مرکز عملیات امنیت[4] در اصل با فعالیتی که انجام می‌دهد تعریف می‌شود؛ یعنی پدافند شبکه رایانه‌ای[5] [۱۱]. پدافند شبکه رایانه‌ای این‌گونه تعریف شده است [۱۲]:

اقداماتی است که برای دفاع در برابر فعالیت‌های غیرمجاز درون شبکه‌های رایانه‌ای اتخاذ می‌شود. پدافند شبکه رایانه‌ای

[1] Reporting
[2] Historical Analysis
[3] Real-time Monitoring and Analysis
[4] Security Operation Center (SOC)
[5] Computer Network Defense (CND)

شامل فعالیت‌های نظارت، تشخیص، تحلیل (از قبیل تحلیل روند و تحلیل الگو)، پاسخ[1] و ترمیم[2] است.

گروهی از خبره‌های امنیت سایبر پدافند شبکه رایانه‌ای را با عبارات بسیاری نام‌گذاری می‌کنند [۱۱]: ازنظر فنی عبارت «گروه پاسخ به رخدادهای امنیت رایانه[3]» صحیح‌ترین واژه‌ای است که می‌تواند به چنین گروهی از افراد اطلاق شود که برای یافتن و پاسخ‌دهی به نفوذها تشکیل شده است؛ اما استفاده عمومی از آن بسیار کم است؛ درنتیجه شناختن آن‌ها از روی نام آن‌ها، همیشه ساده نیست. بسیاری از متخصصان امنیت سایبر، برای نامیدن گروه پاسخ به رخدادهای امنیت رایانه، به‌صورت محاوره‌ای از «مرکز عملیات امنیت» استفاده می‌کنند، درحالی‌که استفاده از واژه مرکز عملیات امنیت، در اینجا نمی‌تواند کاملاً درست باشد؛ اما برای حفظ سازگاری با کاربرد عمومی آن، می‌توان از همان مرکز عملیات امنیت برای نامیدن گروه پاسخ به رخدادهای امنیت رایانه استفاده کرد [۱۱].

در اینجا با ترکیب تعاریف ارائه‌شده از گروه پاسخ به رخدادهای امنیت رایانه ([۱۳-۱۲])، تعریفی از مرکز عملیات امنیت ارائه شده است [۱۱]:

مرکز عملیات امنیت گروهی است که عمدتاً از تحلیل‌گران امنیت تشکیل یافته است و برای تشخیص، تحلیل، پاسخ به، گزارش پیرامون و جلوگیری از رخدادهای امنیت سایبر، سازمان‌دهی شده است.

۲-۲-۱. لایه‌های مرکز عملیات امنیت

یک مرکز عملیات امنیت نوعاً مجموعه‌ای از افراد را اختصاص می‌دهد تا به‌صورت بی‌درنگ، هشدارها را اولویت‌بندی نمایند، همچنین پاسخ تلفن‌های کاربران را بدهند و دیگر کارهای روزمره و عادی را انجام دهند. این گروه غالباً لایه ۱ نامیده می‌شوند. اگر یک هشدار به حد آستانه‌های از پیش تعریف‌شده برسد، لایه ۱ آن را در قالب یک مورد، به لایه ۲ ارجاع می‌دهد. این حد آستانه می‌تواند با توجه به انواع تهدیدهای ممکن (انواع رخدادها، اطلاعات یا تجهیزات هدف‌گزینی شده، مأموریت‌های تحت تأثیر قرارگرفته و غیره) تعریف شود. معمولاً زمان سپری‌شده برای بررسی هر رویداد در لایه ۱ بین یک تا پانزده دقیقه است. که این بستگی به سیاست‌های مرکز عملیات امنیت، مفهوم عملیات، تعداد تحلیل‌گرها، اندازه سازمان و تجهیزات کارفرما و حجم رویدادها دارد. اعضای لایه ۱، علاقه به انجام تحلیل عمیق ندارند چون آن‌ها نباید رویدادهای ورودی از منابع بی‌درنگ را از دست بدهند. اگر ارزیابی رویدادی بیش از چند دقیقه زمان بگیرد، به لایه ۲ ارجاع می‌شود [۱۱].

در لایه ۱، دو خدمت اصلی ارائه می‌شود [۱۱]:

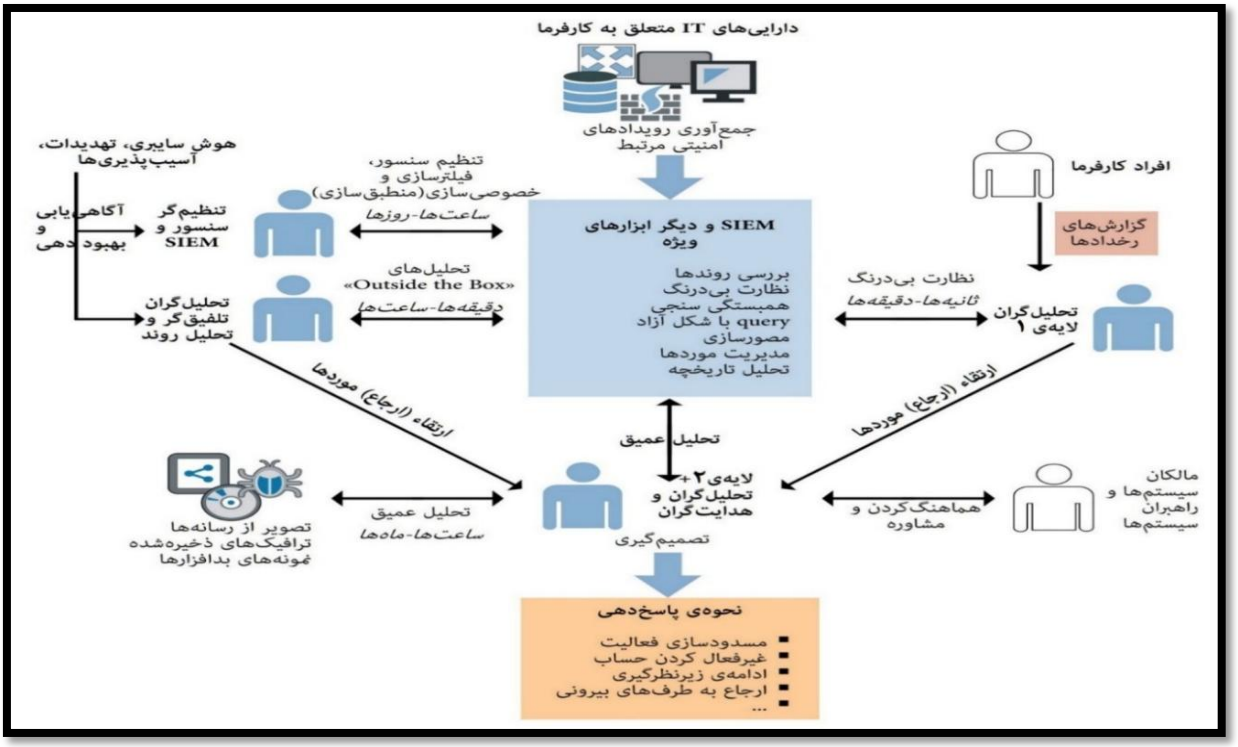
۱. مرکز تماس: این مرکز به دریافت نکات و اطلاعات، گزارش رخدادها و درخواست خدمات پدافند شبکه رایانه‌ای از اعضای کارفرما از طریق تلفن، رایانامه، وب سایت مرکز عملیات امنیت یا دیگر روش‌ها می‌پردازد.
۲. نظارت بی‌درنگ و اولویت‌بندی: انجام اولویت‌بندی و تحلیل‌های کوتاه‌مدت در مورد داده‌های بی‌درنگ ورودی (مثل هشدارها و ثبت رویدادهای سیستمی) برای یافتن نفوذهای ممکن.

لایه ۲ موارد ارسالی از لایه ۱ را دریافت می‌کند و تحلیل عمیق روی آن انجام می‌دهد تا تعیین نماید که واقعاً چه اتفاقی رخ داده است (تا جایی که ممکن است و زمان و داده‌های موجود اجازه دهد) و اینکه چه اقدامات دیگری لازم است. پیش از اتخاذ این تصمیم، ممکن است جمع‌آوری و رسیدگی به تمام داده‌های ضروری برای تعیین وسعت و شدت رویداد، چند هفته زمان ببرد. ازآنجاکه لایه ۲ مسئول نظارت بی‌درنگ نیست و همچنین تحلیل‌گرانی باتجربه‌تر در اختیار دارد، می‌تواند زمان کافی برای تحلیل کامل هر مجموعه فعالیت، جمع‌آوری اطلاعات بیشتر و هماهنگی با کارفرما، اختصاص دهد. تعیین وقوع یک رخداد بالقوه، به طور معمول مسئولیت لایه ۲ (یا بالاتر) است [۱۱].

۲-۲-۲. نقش‌های موجود در مرکز عملیات امنیت

برای تشریح تمام نقش‌های موجود در بخش‌های مختلف مرکز عملیات امنیت، باید دانست که هر مرکز عملیات امنیت نقش‌ها را به‌صورتی متفاوت تقسیم می‌کند و همچنین بین کارکردهای مختلف می‌تواند همپوشانی وجود داشته باشد. برخی مراکز عملیات امنیت تحلیل عمیق و پاسخ‌دهی را در یک لایه یکسان (لایه ۲) انجام می‌دهند. برخی دیگر، بعضی از این کارکردها را به سه لایه تقسیم می‌کنند [۱۱]. نقش‌ها و مسیر ارجاع‌ها در یک مرکز عملیات امنیت به‌صورت عام در شکل (۱) نشان داده شده است:

[1] Response
[2] Restoration
[3] Computer Security Incident Response Team (CSIRT)



شکل (۱): نقش‌ها و مسیر ارجاع رخدادها در مرکز عملیات امنیت [۱۱]

۳. بررسی سامانه‌های موجود

برای ارزیابی فنی سامانه‌های مرکز عملیات امنیت، شش شاخص فنی در نظر گرفته شده است که به شرح زیر است:

- بخش مدیریت رویداد
- بخش تحلیل رویداد
- بخش پایگاه دانش
- بخش داشبورد
- بخش حسگر
- بخش ارائه خدمات امنیتی مدیریت‌شده[1] (MSSP)

در این مقاله تمرکز اصلی روی بخش داشبورد بوده است که این بخش نیز شامل قسمت‌های مختلفی است که فهرست آن‌ها در پایین آمده است:

- تنوع روش‌های پیکربندی رابط گرافیکی و خط فرمان
- امکان گزارش‌گیری و مدیریت تغییرات روی زیرسامانه‌های مرکز عملیات امنیت
- یکپارچگی، جامعیت و کفایت رابط گرافیکی
- امنیت رابط کاربری
- تنوع داشبوردها
- کیفیت داشبوردها به لحاظ برخط بودن، بی‌درنگ بودن، فیلتر کردن و غیره
- کفایت گزارش‌هایی از قبیل بدافزارها، فعالیت‌های شبکه، امکان گزارش‌گیری به‌صورت زمان‌بندی‌شده و غیره

در این تحقیق، سامانه‌های تجاری زیر بر اساس ویژگی‌های مختلف آنها مورد بررسی قرار گرفت:

- محصول تجاری شرکت HP (ArcSight ESM v4.5)
- محصول تجاری شرکت IBM (QRadar SIEM)
- سامانه همبسته‌ساز هشدار پرهام
- سامانه مدیریت اطلاعات و رخدادهای امنیتی راوین
- محصول کورلاگ
- محصول سیترا

که پس از بررسی مستندات فنی برای محصولات خارجی و مقایسه فنی پس از نصب و راه‌اندازی به‌صورت آزمایشی برای محصولات بومی، در جدول زیر مقایسه بخش داشبوردها آمده است. گفتنی است در جدول (۱) مقدار کارایی بر پایه عدد ۵ است که هرچه عدد نسبت داده‌شده به ۵ نزدیک‌تر باشد، محصول

[1] Managed Security Service Provider

میزان کارایی و رضایت‌مندی بالاتری را نشان می‌دهد.

جدول (۱): مقایسه بخش داشبورد محصولات

نام محصول	میزان کارایی (در مقیاس ۱ تا ۵)
Qradar	۴/۳
ArcSight	۴
پرهام	۳/۹۳
راوین	۲/۳۵
کورلاگ	۲/۲۴
سیترا	۲/۱۹

۳-۱. تحلیل و بررسی

برای ایجاد یک مرکز پدافند سایبری، نیروی انسانی متخصص، ابزارها و روال‌ها از اجزای اصلی تشخیص‌دهنده این مرکز هستند که تقریباً ۷۰٪ کار این مرکز با نیروی انسانی متخصص است و صرفاً ۳۰٪ مابقی آن مربوط به ابزارها و روال‌هاست، بنابراین، احتمال خطای نیروی انسانی متخصص در شرایط مختلف وجود خواهد داشت.

با توجه به اینکه نیروی انسانی در شرایط مختلف می‌تواند تأثیرات متفاوتی در واکنش به تهدیدات سایبری داشته باشد، برای کاهش تأثیرات متفاوت و ارتقای امنیت و پدافند سایبری، باید راه‌حل‌هایی در مرکز عملیات امنیت استفاده کرد. گفتنی است در بررسی تمامی محصولات مرکز عملیات امنیت بومی و غیربومی، برای کاهش خطای نیروی انسانی در مرکز پدافند سایبری، مؤلفه خاصی پیشنهاد نشده است. با بررسی و جمع‌بندی سامانه‌های مرکز عملیات امنیت موجود شامل سامانه‌های داخلی و خارجی، نتیجه‌گیری شد که مصورساز بی‌درنگ حملات سایبری در بین مصورسازهایی که مرکز عملیات امنیت در اختیار تحلیل‌گران قرار می‌دهد، وجود ندارد. بنابراین، استفاده از این مصورساز برای تحلیل‌گران مرکز عملیات امنیت موضوعی جدید و قابل‌طرح است که به کاهش خطای نیروی انسانی و افزایش سرعت عملکرد آن کمک می‌کند.

۴. روش پیشنهادی

در حملات سایبری به شبکه لازم است یک دفاع یکپارچه در مقابل تهدیدات و حملات سایبری در نظر گرفته شود و آن در صورتی محقق خواهد شد که یک مرکز پدافند سایبری ایجاد شود. در مرکز پدافند سایبری تحلیل‌گر با دیدن وضعیت حملات سایبری به‌صورت بی‌درنگ و استفاده از این داده‌ها در کنار دیگر داده‌های موجود، بتواند به‌صورت زودهنگام برای تغییر در سیاست‌ها و پیکربندی‌ها، نتیجه‌گیری نماید و آن را به راهبران سامانه‌ها و شبکه‌ها اعلام نماید. بدین منظور، روش مصورساز پدافند سایبری این است که در کنار اطلاعات و ابزارهایی مثل سامانه مدیریت رویداد و اطلاعات امنیتی[1] که در اختیار تحلیل‌گر قرار دارد و در کنار مصورسازهایی که در اختیار او هست، یک مصورساز بی‌درنگ حملات سایبری، استفاده شود. روش مصورساز پدافند سایبری (مُپسا) کمک می‌کند تا تحلیل‌گر بتواند اطلاعات گذشته و غیر بی‌درنگ را با داده‌های بی‌درنگ مربوط به وضعیت حملات، مقایسه کرده و نتیجه‌گیری‌های زودهنگام برای نیاز به تغییر در سیاست‌ها و پیکربندی‌ها را انجام دهد و به متخصصین مربوطه اطلاع دهد.

۴-۱. لایه‌ها و نقش‌ها در مُپسا

با توجه به استانداردهای مرکز عملیات امنیت، ۱۶ بخش اصلی در مرکز عملیات امنیت وجود دارد. دو بخشی که در اینجا اهمیت دارد، بخش داشبورد و بخش مشورت امنیتی است. در روش مُپسا این دو بخش بهبود داده شده است. همان‌طور که در فصل قبل بیان شد، در بین داشبوردها و مصورسازهای مراکز عملیات امنیت فعلی، مصورساز بی‌درنگ حملات سایبری وجود ندارد که در روش مُپسا این مؤلفه اضافه می‌گردد. از طرفی همان‌طور که در شکل (۱) دیده می‌شود مشورت‌های امنیتی برای تغییرات زودهنگام از طریق لایه ۱ به راهبران سامانه‌ها و شبکه‌ها وجود ندارد که با مؤلفه پیشنهادی، این مسیر قرار داده می‌شود.

لایه‌ها و نقش‌ها در مُپسا به همان صورتی است که در یک مرکز عملیات امنیت به‌صورت عام وجود دارد (شکل ۱). تفاوت اصلی مُپسا با یک مرکز عملیات امنیت معمولی از این نظر در مسیر ارجاع‌ها است. هر مرکز عملیات امنیت حداقل ۲ لایه از تحلیل‌گران را در اختیار دارد، همان‌طور که بیان شد، لایه ۱ وظیفه نظارت بی‌درنگ و پیوسته و بررسی‌های سریع و زودهنگام را دارد و لایه ۲، وظیفه تحلیل‌های عمیق و طولانی‌مدت را بر عهده دارد. بر اساس شکل (۱)، معماری مُپسا در شکل (۲) نشان داده شده است.

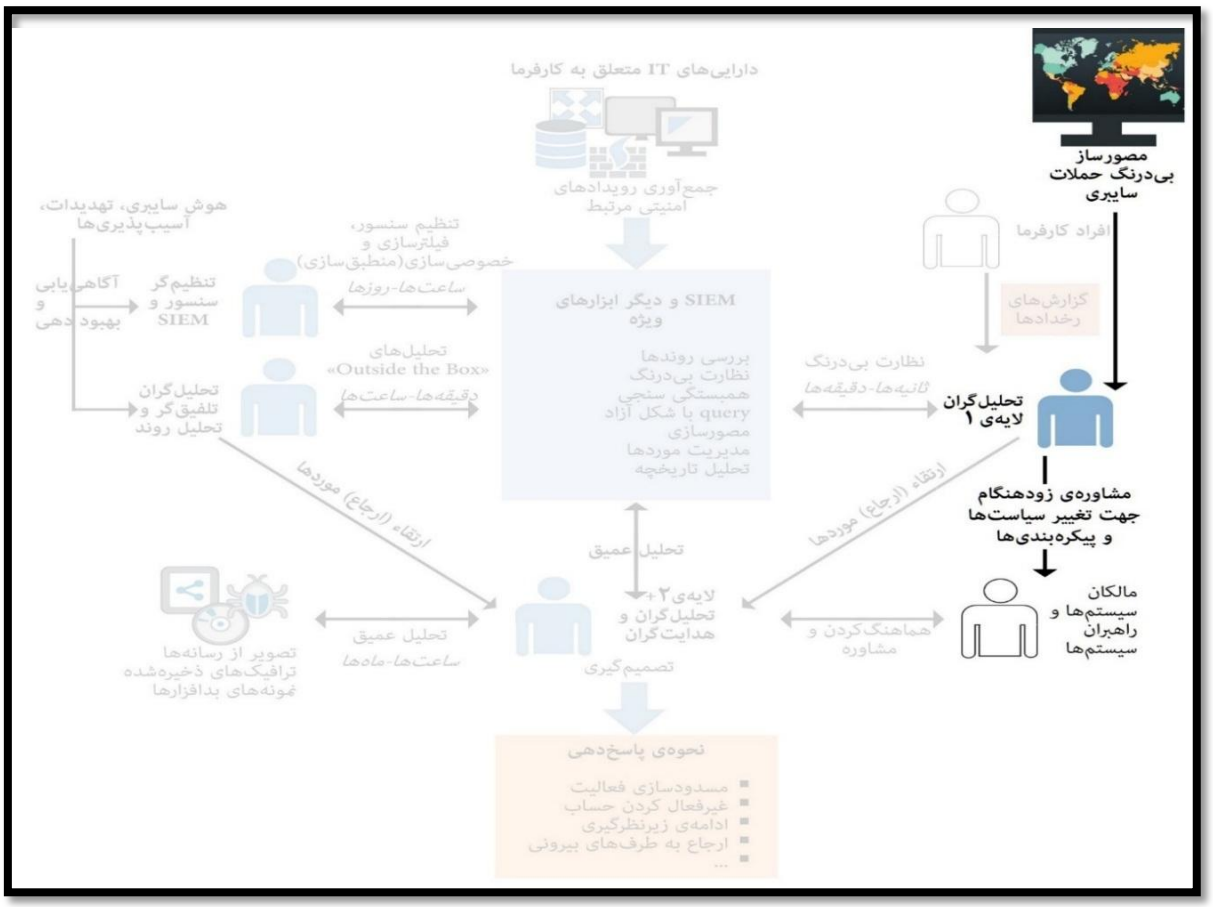
در مرکز عملیات امنیت معمولی، مسیری برای مشاوره زودهنگام به راهبران هنگام نیاز به تغییرات آنی وجود ندارد و مشاوره‌ها از طریق لایه ۲ صورت می‌گیرد که معمولاً مشاوره‌هایی با گذر زمان هستند. اما اگر بتوان به‌صورت زودهنگام به راهبران پیشنهاد تغییرات در پیکربندی‌های سامانه‌ها و شبکه‌ها را ارائه کرد، می‌توان موجب کاهش یا حذف اثر حملات گردید.

[1] Security Information and Event Management (SIEM)

در یک شبکه گسترده از نظر جغرافیایی که در سراسر کشور گسترده است، شناسایی تغییر وضعیت حملات به نقاط مختلف شبکه و دیدن حملات به‌صورت بی‌درنگ بسیار ضرورت دارد. با در اختیار داشتن این اطلاعات، به‌سرعت می‌توان در موردنیاز به ایجاد تغییر در پیکربندی‌های سامانه‌ها و شبکه‌ها، تصمیم‌گیری کرد تا از نشت اطلاعات ناشی از این حملات جلوگیری شود یا اثر آن کاهش داده شود. بنابراین، یکی از داده‌هایی که باید مورد نظارت بی‌درنگ تحلیل‌گران شبکه‌های گسترده قرار بگیرد، داده‌های حملات بی‌درنگ است. بهترین و اثربخش‌ترین حالت نمایش این داده‌ها، استفاده از یک مصورساز برای به تصویر کشیدن این داده‌ها به‌صورت بی‌درنگ است تا تحلیل‌گر به‌صورت بی‌درنگ متوجه تغییرات آن شود و با استفاده از دیگر اطلاعات و داده‌هایی که در اختیار دارد بتواند به‌صورت زودهنگام تصمیم‌گیری نماید.

بررسی مراکز عملیات امنیت تجاری موجود در بازار، نشان داد که هیچ‌کدام از آن‌ها، چنین مصورسازی را استفاده نمی‌کنند. بنابراین، در مُپسا، مصورساز بی‌درنگ حملات، در کنار دیگر مصورسازها در اختیار تحلیل‌گران لایه ۱ قرار می‌گیرد. تحلیل‌گران لایه ۱ با بررسی دیگر داده‌ها و نظارت پیوسته بر حملات سایبری، می‌توانند در صورت نیاز، راجع به نیاز به تغییر در سیاست‌ها و پیکربندی‌ها، به سرعت تصمیم‌گیری نمایند.

نتیجه‌گیری‌های زودهنگام تحلیل‌گران لایه ۱ به‌صورت مستقیم در قالب مشاوره، به راهبران سامانه‌ها، شبکه‌ها و ابزارهای جلوگیری از نشت اطلاعات، اطلاع داده می‌شود. به‌عنوان‌مثال مشاهده افزایش حملات در یک جغرافیای خاص یا وقوع نوعی از حمله در یک نقطه از شبکه، نتیجه می‌دهد که باید برای کاهش آسیب آن، تغییراتی در تجهیزات شبکه از قبیل مسدودسازی IP یا یک خدمت خاص اعمال نمود. بدین ترتیب، تغییرات لازم به‌صورت زودهنگام، اعمال می‌شود تا نشت اطلاعات ناشی از حملات به حداقل برسد یا از آن جلوگیری شود.



شکل (۲): اضافه کردن مصورساز بی‌درنگ حملات سایبری به مرکز عملیات امنیت

۴-۲. کاربردهای مُپسا

آمارها حاکی از آن است که حملات علیه شبکه‌های گسترده، رشد چشمگیری داشته است. امروزه، با افزایش خدمات الکترونیکی و پیشرفت حملات سایبری، روش‌های قدیمی کارایی خود را از دست داده‌اند و نیاز جدی‌تری به روش‌های ترکیبی احساس می‌شود. لذا ضروری است که سازمان‌ها یک رویکرد پیشگیرانه برای مواجهه با تهدیدات سایبری در پیش گیرند. بنابراین، مصورسازی حملات سایبری توزیع‌شده می‌تواند در این امر مؤثر باشد این‌روش که به‌عنوان یک مؤلفه در مرکز عملیات امینت سایبری اضافه می‌شود کمک می‌کند تا بتوان دفاع یکپارچه را در برابر تهدیدات نوین، برنامه‌ریزی و اجرایی نمود. خلاصه این‌که مُپسا برای افزایش امنیت شبکه‌های گسترده ارائه شده است.

البته این نکته قابل‌توجه است که در بخش‌های حیاتی نظیر انرژی، حمل‌ونقل، دفاعی و سلامت عمومی به‌منظور پیشگیری و دفاع در برابر تهدیدات و حملات سایبری، روش ارائه‌شده می‌تواند مورداستفاده قرار گیرد.

۴-۳. طرح پیاده‌سازی مُپسا

داده‌های این مصورساز توسط حسگرهایی که در نقاط مختلف شبکه توزیع‌شده هستند، تأمین می‌شود. در مورد سازمانی که در کل کشور شعبه دارد و شبکه آن در کل کشور توزیع شده است، همان‌طور که در شکل (۳) دیده می‌شود، می‌توان اطلاعات حسگرهای قرار گرفته در استان‌های مختلف را جمع‌آوری کرده و به مرکز داده‌ی مستقر در مرکز، انتقال داد و برای نمایش بی‌درنگ حملات سایبری شناسایی‌شده توسط حسگرها از آن‌ها استفاده کرد.

شکل (۳): توزیع حسگرها به‌صورت نمونه

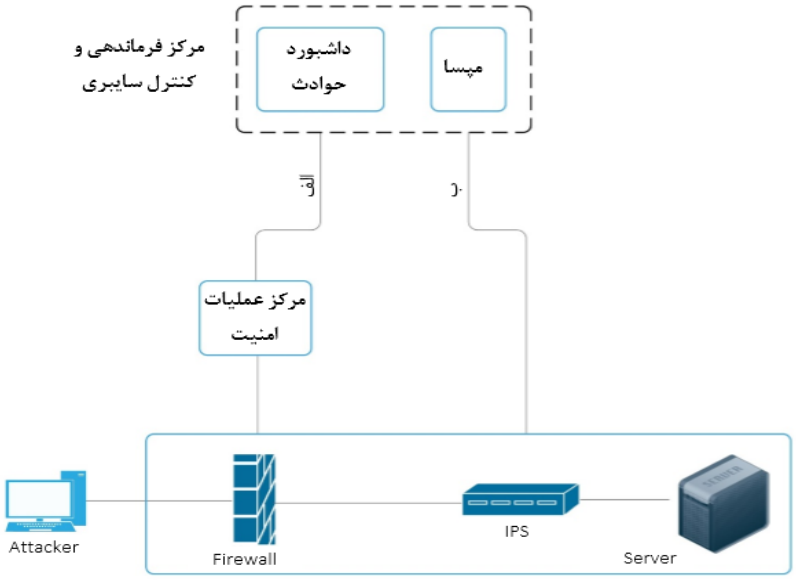
۴-۴. پیاده‌سازی نسخه آزمایشگاهی مُپسا

برای پیاده‌سازی راه‌کار مُپسا، معماری زیر شبیه‌سازی شده است. در این معماری دو مسیر مشاهده می‌شود. در مسیر *الف*، رخدادهای امنیتی توسط سامانه‌های دیواره آتش و مدیریت رویداد و اطلاعات امنیتی تشخیص داده شده و از طریق مرکز عملیات امنیت برای مرکز فرماندهی و کنترل دفاع سایبری ارسال می‌گردد و در داشبورد حوادث مرکز نمایش داده می‌شود. در مسیر ب، رخدادهای امنیتی از طریق حسگر سامانه تشخیص و جلوگیری از نفوذ تشخیص داده شده و به‌صورت مستقیم برای ابزار مصورسازی مُپسا در مرکز فرماندهی و کنترل دفاع سایبری ارسال می‌شود. همان‌طور که در شکل (۴) مشاهده می‌شود مهاجم در این معماری دو حمله Port Scan و Command Execution را اجرا می‌کند. حمله اول توسط هر دو مسیر تشخیص داده می‌شود و حمله دوم تنها توسط مسیر مُپسا تشخیص داده می‌شود.

در شکل (۵) نسخه آزمایشی نرم‌افزار AttackMap از دو بخش سرور و کلاینت وب تشکیل شده است. چارچوب توسعه بخش سرور، Java Spring MVC است. محیط توسعه، Jetbrains IntelliJ IDEA 2016 است که بر اساس سیستم Build اختصاصی Maven نرم‌افزار را به‌صورت Web Archive روی Tomcat مستقر می‌کند. وظیفه بخش سرور به شرح زیر است:

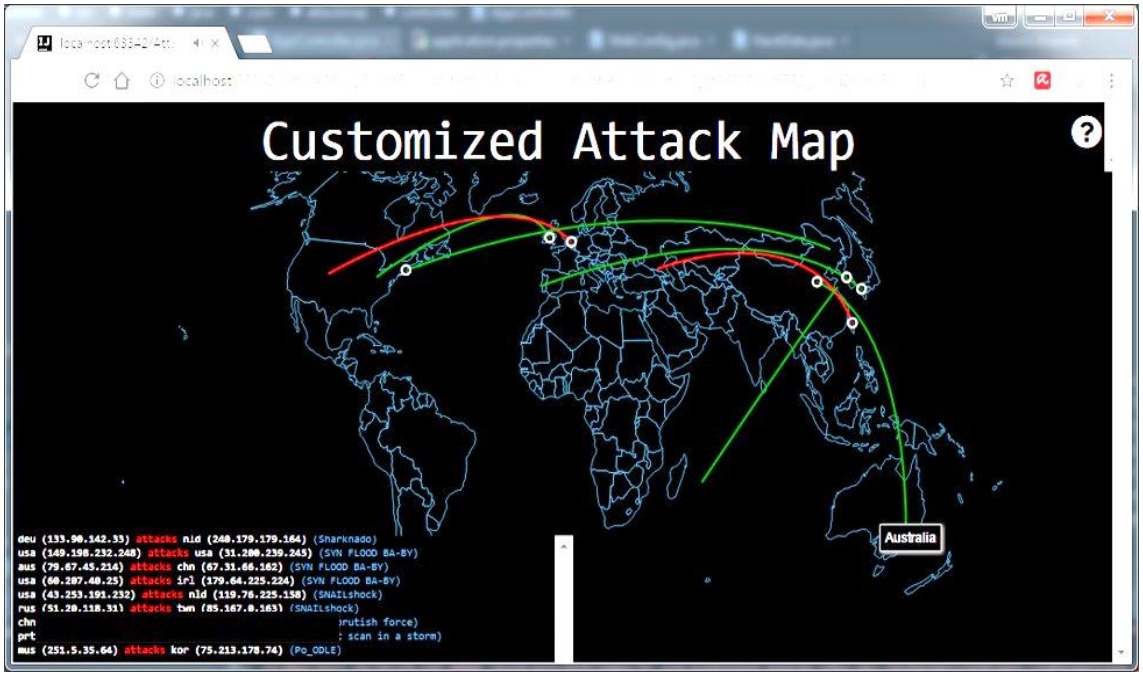
- دریافت دوره‌ای اطلاعات موارد حمله شامل آدرس IP مبدأ و مقصد و نوع دسته‌بندی حمله
- تعیین جغرافیایی آدرس‌های IP مبدأ و مقصد
- تحلیل آماری و تجمیعی حملات بر اساس دسته‌بندی
- تشکیل اطلاعات JSON لازم برای نمایش گرافیکی لحظه‌به‌لحظه
- ارسال اطلاعات جدید در قالب سرویس وب REST به کلاینت وب

کلاینت وب مبتنی بر Angular JS بوده و چارچوب توسعه آن Node.js است و از کتابخانه D3.js برای خروجی گرافیکی استفاده شده است. در حال حاضر این کلاینت فقط قابلیت نمایش مبدأ و مقصد حمله از روی اطلاعات دریافتی سمت سرور را داشته و بسته به نوع دسته‌بندی حمله، رنگ متفاوتی برای اتصال مبدأ به مقصد حمله در نظر می‌گیرد که البته قابلیت ایجاد نمودارهای مختلف در اطراف آن برای نتایج تحلیل‌های مختلف وجود دارد. شکل (۵) نمایی از نتیجه اجرا را نشان می‌دهد:



شکل (۴): طرح پیاده‌سازی راه‌کار مُپسا

کلاینت وب، بر اساس داده‌های جغرافیایی، نگاشت بین نقطه مبدأ و نقطه مرکز آن را روی نقشه انجام می‌دهد و نمایش کمان نشانگر حمله از این نقطه متصل می‌شود. به‌عنوان‌مثال نقشه مبدأ به مقصد حملات در شکل (۵) آمده است:



شکل (۵): نمایی از خروجی نرم‌افزار AttackMap

۵. ارزیابی روش پیشنهادی

در این بخش، پیاده‌سازی و استقرار عملی راه‌کار مُپسا ارائه شده است. معیارهایی که برای ارزیابی این‌روش، در نظر گرفته شده است، همان اهداف تعریف‌شده برای تحقیق است که ازجمله آن‌ها، تشخیص بی‌درنگ حملات سایبری، کاهش خطای نیروی انسانی و افزایش سرعت تصمیم‌گیری می‌باشد؛ یعنی هرچه، تحقق اهداف بیشتر صورت گرفته باشد، راه‌کار مُپسا، بهینه بودن عنوان اصلی تحقیق است را بیشتر محقق خواهد کرد.

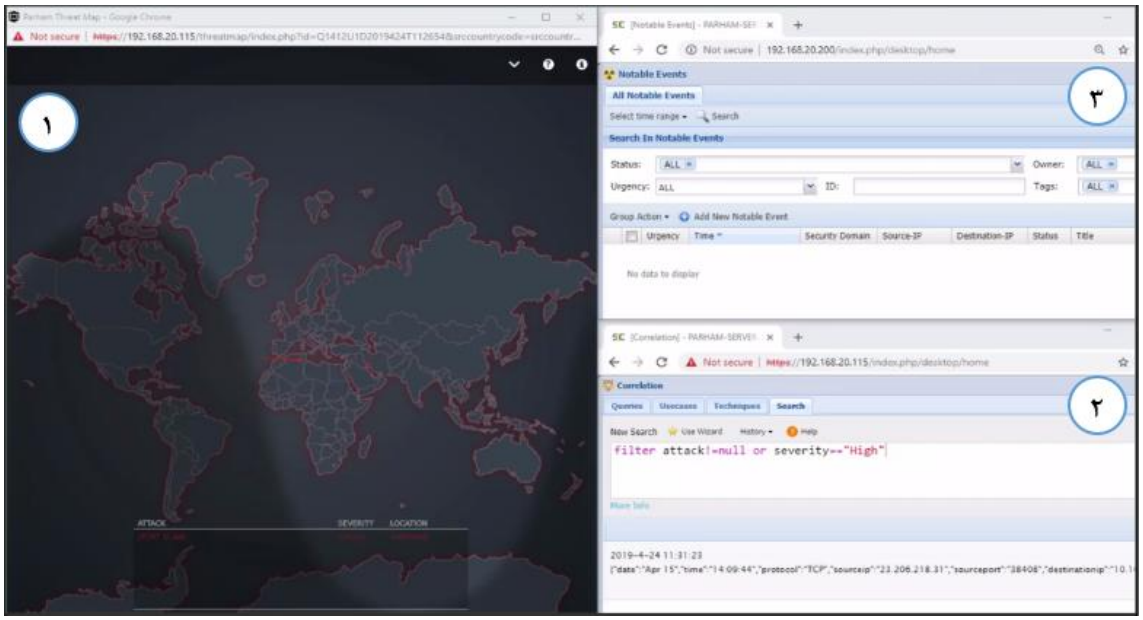
در حمله اول (Port Scan) هر دو مسیر *الف* و مسیر *ب* حمله را تشخیص داده و در مرکز فرماندهی و کنترل دفاع سایبری مشاهده می‌شود. شکل (۶) از سه بخش تشکیل می‌شود:

بخش اول: ابزار مصورسازی مُپسا در مرکز فرماندهی و کنترل

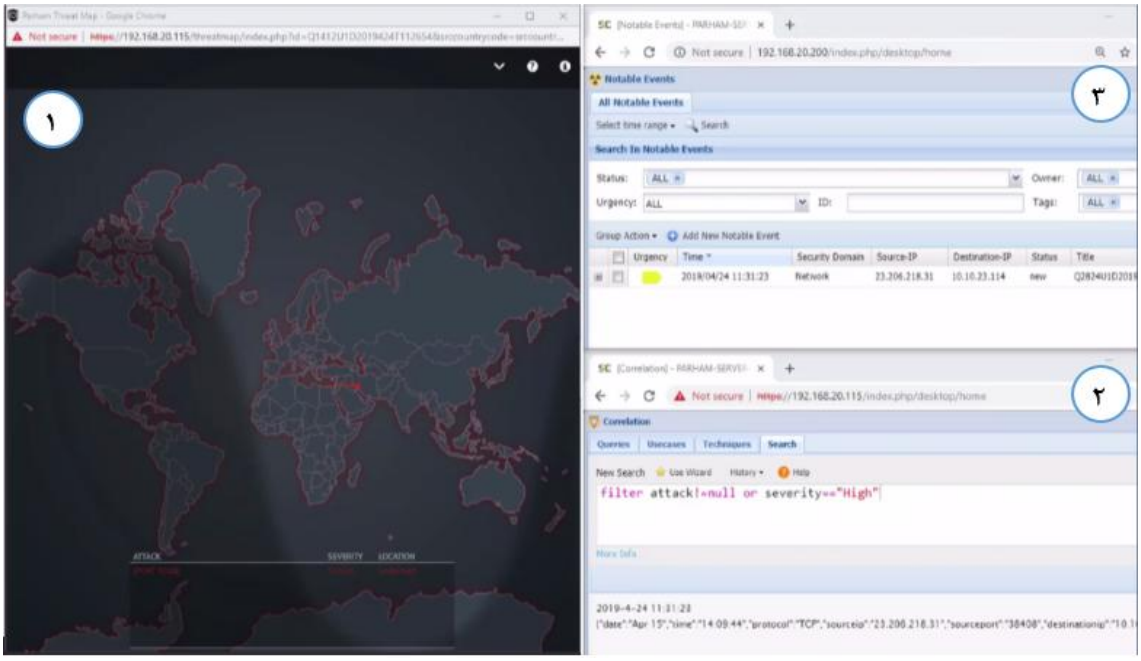
بخش دوم: مرکز عملیات امنیت

بخش سوم: داشبورد حوادث در مرکز فرماندهی و کنترل سایبری

همان‌طور که در شکل (۶ و ۷) مشاهده می‌شود حمله هم‌زمان با مرکز عملیات امنیت در نقشه به‌صورت گرافیکی در مرکز فرماندهی و کنترل دفاع سایبری نمایش داده می‌شود. در این زمان هنوز داشبورد رخداد حمله را نمایش نداده است (حمله پس از گذشت ۲ ثانیه در داشبورد رخداد مشاهده می‌شود). در نتیجه می‌توان گفت که راه‌کار مُپسا می‌تواند سرعت دریافت حادثه در مرکز فرماندهی و کنترل دفاع سایبری را افزایش دهد. از طرفی شیوه مُپسا اثربخشی بسیار بالاتری نسبت به داشبوردهای متداول مورد استفاده در بخش سوم شکل (۶) را دارد.



شکل (۶): نمایش حمله سایبری در مُپسا

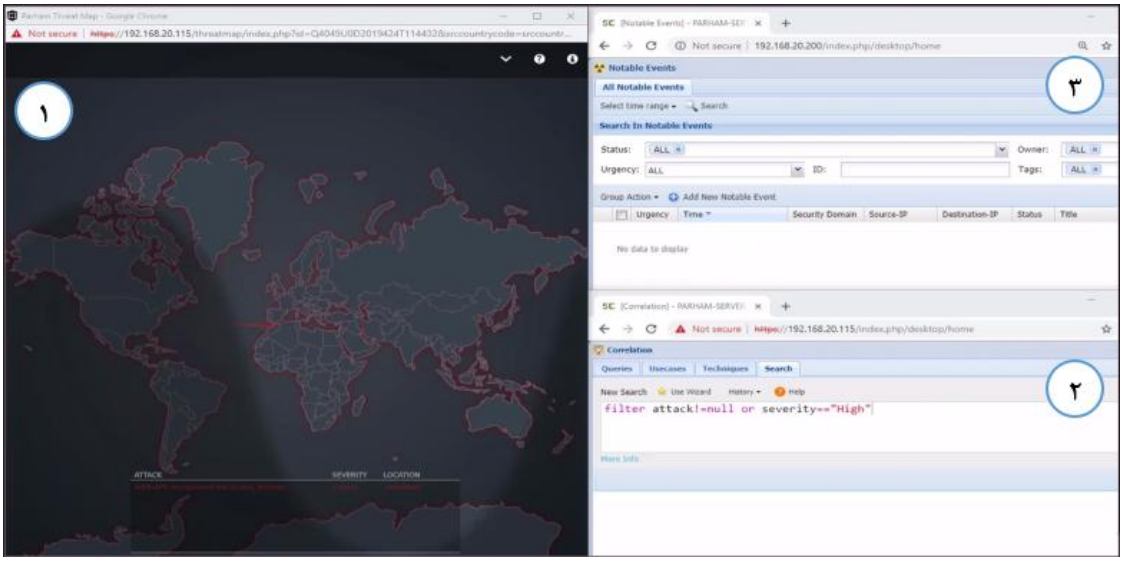


شکل (۷): نمایش حمله سایبری پس از ۲ ثانیه در داشبورد حوادث

همان‌طور که در شکل (۸) مشاهده می‌شود حمله دوم (Command Execution) تنها توسط مسیر مُپسا شناسایی می‌شود. از این‌رو اگر سازمان‌ها از نظر بلوغ و حسگرهای امنیتی به حدی نرسیده باشند که بتوانند حملات مختلف را تشخیص دهند، راه‌کار مُپسا با پوشش تجهیزات امنیتی می‌تواند این‌گونه حملات را نیز شناسایی کرده و لذا از این نظر بر مسیر

الف برتری دارد.

مطابق جدول (۲) به غیر از بند دوم شاخص‌های ارزیابی مسیر *الف* و مسیر ب، در تمامی شاخص‌های مطرح‌شده، مسیر ب که همان روش مُپسا می‌باشد، نسبت به مسیر *الف* بهبود یافته است. بنابراین، می‌توان نتیجه گرفت در مسیر ب که از روش مُپسا استفاده می‌شود، تشخیص رخدادهای ناشی از حملات سایبری مطابق با معماری پیاده‌سازی در شکل (۴)، بهبود یافته است. در یک جمع‌بندی می‌توان به این نتیجه رسید که این سازوکار (مصورسازی بی‌درنگ حملات سایبری) باعث کاهش خطای نیروی انسانی متخصص و در نهایت بهبود تشخیص رخداد در مرکز پدافند سایبری خواهد شد.



شکل (۸): نمایش شناسایی حمله سایبری تنها توسط مُپسا

جدول (۲): مقایسه مسیر الف و مسیر ب با توجه به شاخص‌ها

ردیف	شاخص‌ها	مسیر الف	مسیر ب (روش مُپسا)
۱	شناسایی حمله در سطح ترافیک شبکه	n	n+1
۲	شناسایی حمله در سطح رویداد شبکه	n	n-1
۳	سرعت تشخیص حمله	n	n+1
۴	هزینه نصب و راه‌اندازی	n	n-1
۵	تعداد نیروی انسانی متخصص	n	n-1
۶	زمان میزان‌سازی تجهیزات فعال	n	n-1
۷	اثربخشی با رویکرد کاهش خطای نیروی انسانی	n	n+1

۶. نتیجه‌گیری

هدف اصلی این تحقیق، ارائه یک روش بهبودیافته تشخیص رخداد ناشی از حملات سایبری و جلوگیری از نشت اطلاعات ناشی از آن بوده است. بر این اساس، در مراحل انجام تحقیق حوزه‌های مصورسازی، سامانه همبستگی‌سنجی رویدادها، مرکز عملیات امنیت و همچنین بررسی و مقایسه محصولات تجاری موجود مورد بررسی قرار گرفت.

در روند تحقیق، این نتیجه حاصل شد که برای کاهش یا جلوگیری از نشت اطلاعات ناشی از حملات سایبری، راه‌کاری که وجود دارد آن است که حملات واقع‌شده، به‌صورت بی‌درنگ مورد نظارت قرار بگیرد تا پیش از ایجاد و گسترش اثرات مخرب آن، بتوان در مورد تغییرات موردنیاز در پیکربندی سامانه‌ها و شبکه‌ها، تصمیم‌گیری سریع اتخاذ گردد. مرکز اصلی نظارت و پایش شبکه، مرکز عملیات امنیت است. با بررسی و جمع‌بندی حاصل‌شده بر نمونه‌های تجاری موجود، مشخص شد که هیچ‌کدام از آن‌ها نظارت بی‌درنگ بر حملات را به متصدیان خود ارائه نمی‌دهند تا آن‌ها بتوانند به‌سرعت در مورد آن تصمیم‌گیری نمایند.

بر همین اساس، روش پیشنهادی حاصل از این تحقیق (مُپسا) آن است که یک ابزار مصورساز بی‌درنگ حملات سایبری نیز در بین مصورسازهای مرکز عملیات امنیت قرار داده شود تا تحلیل‌گر مربوطه، با توجه به آن و با در نظر گرفتن دیگر داده‌هایی که در دست دارد، در مورد تغییرات موردنیاز در پیکربندی شبکه‌ها و سامانه‌ها تصمیم‌گیری نموده و آن را به اطلاع راهبران سامانه‌ها و شبکه‌ها قرار دهد تا آن‌ها تغییرات موردنیاز را اعمال نمایند.

از نوآوری‌های این تحقیق می‌توان به موارد زیر اشاره نمود:

- بهبود نظارت و پایش در مرکز عملیات امنیت
- استفاده از مصورساز بی‌درنگ در کنار داده‌ها و مصورسازهای تاریخچه‌ای

۶-۱. چالش‌ها

با توجه به این‌که مُپسا قرار است به‌عنوان یک مؤلفه در مرکز پدافند سایبری اضافه شود به‌طور یقین چالش‌هایی برای پیاده‌سازی وجود دارد که به شرح زیر است:

۱. لازم است در مؤلفه بیان‌شده انواع فرمت داده‌ها که از حسگرهای مختلف تولید می‌شود قابل‌فهم برای این مؤلفه باشد.

۲. با توجه به این‌که در شبکه‌های گسترده با حجم زیادی از داده‌ها برخورد می‌شود، لازم و ضروری است برای این حجم از داده‌ها تفکر و تصمیم جدی گرفته شود.

۳. برای مسئله داده‌های بزرگ[1] و تحلیل آماری آن‌ها، باید راه‌کار مناسبی و با نگاه علمی به آن اندیشید.

۴. در خصوص معماری پیاده‌سازی آن به لحاظ متمرکز بودن و یا توزیع‌شدگی، به‌صورت دقیق بررسی فنی صورت گیرد.

۶-۲. پیشنهادهای آینده

به‌منظور توسعه تحقیق حاضر، عناوین و موضوعات زیر برای تحقیقات آینده پیشنهاد می‌گردد:

- در مُپسا صرفاً به مصورساز پرداخته شد اما برای ارائه اطلاعات دقیق‌تر و تصمیم‌گیری بهتر، پیشنهاد می‌شود از تحلیل‌های آماری استفاده شود و در اختیار تحلیل‌گر قرار داده شود.
- خطر مهم دنیای سایبر در حال حاضر تهدیدات پیشرفته پایدار هستند که برای مقابله با آن‌ها هنوز راه‌حل‌های قطعی و جامع وجود ندارد. یکی از زمینه‌های مهم تحقیقاتی، تحقیق پیرامون راه‌حل‌های مقابله با تهدیدات پیشرفته پایدار با رویکرد دفاع یکپارچه است. که مؤلفه مصورسازی دقیق می‌تواند یکی از موضوعات اساسی برای این‌رویکرد باشد.

[1] Big-Data

۷. مراجع

[1] Z. Li, Q. Liao, and A. Striegel, Botnet Economics: Uncertainty Matters," In Managing Information Risk and the Economics of Security, M. E. Johnson, Ed., Boston, Springer US, pp. 245-267, 2009.

[2] J. Baltazar, J. Costoya, and R. Flores, "The Heart of KOOBFACE C&C and Social Network Propagation," Trend Micro, Inc., 2009.

[3] T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling, "Measurements and mitigation of peer-to-peer-based botnets: A case study on stormworm," In Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, San Francisco, 2008.

[4] A. Caglayan, M. Toothaker, D. Drapaeau, D. Burke, and G. Eaton, "Behavioral analysis of fast flux service networks," In Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Oak Ridge, 2009.

[5] D. Andriesse, C. Rossow, B. Stone-Gross, D. Plohmann, and H. Bos, "Highly Resilient Peer-to-Peer Botnets Are Here: An Analysis of Gameover Zeus," In MALWARE, 2013.

[6] A. D'Amico, L. Buchanan, D. Kirkpatrick, and P. Walczak, "Cyber Operator Perspectives on Security Visualization," In Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, Walt Disney World, Florida, USA, 2016.

[7] L. Buchanan, A. D'Amico, and D. Kirkpatric, "Mixed method approach to identify analytic questions to be visualized for military cyber incident handlers," In IEEE Symposium on Visualization for Cyber Security (VizSec), Baltimore, MD, USA, 2016.

[8] J. Garae and R. K. L. Ko, "Visualization and Data Provenance Trends in Decision Support for Cybersecurity," Data Analytics and Decision Support for Cybersecurity, pp. 243-270, 2017.

[9] R. Marty, "Applied Security Visualization," 1 ed., Boston: Addison Wesley Professional, 2008.

[10] S. Few, "Information Dashboard Design: The Effective Visual Communication of Data," 1st ed., C. Wheeler, Ed., O'Reilly, 2006.

[11] C. Zimmerman, "Ten Strategies of a World-Class Cybersecurity Operations Center," McLean: MITRE Corporation, 2014.

[12] Committee on National Security Systems, "Committee on National Security Systems (CNSS) Glossary, CNSSI no. 4009," Committee on National Security Systems, 2015.

[13] N. Brownlee and E. Guttmanm, "Expectations for Computer Security Incident Response, RFC 2350," 1998.

Journal of Electronical & Cyber Defence
Vol. 7, No. 4, 2020, Serial No. 28

An Improved Method of Incident Detection due to Cyber Attacks

M. H. HassanNia, M. R. HasaniAhangar*, A. Gafori

*Imam Hossein Comprehensive University

(Received: 04/12/2018, Accepted: 18/06/2019)

ABSTRACT

Human errors in design and configuration of networks and systems are potentials for attacks. Security Operation Center often used in wide networks, is a solution for continuous monitoring and detection, and human workers have key role in it. Through study of visualization subject and comparison between commercial samples of SOCs, this paper proposed a method that helping early detection in wide networks. The proposed method (MAPSA) is adding a cyber-attack real-time visualization module in SOC which SOC's analyzers may use it to early decide about modifications requirement in networks. This method leads to human error reduction, growth of personnel's effectiveness and increase in speed of modification. Therefore decreases the effects of attacks on wide networks.

Keywords: Security operation center, Visualization, Real-time, Cyber-attacks

* Corresponding Author Email: mrhasani@ihu.ac.ir