فصلنامهٔ امنیت پژوهی (علمی-پژوهشی)
سال بیست‌وسوم: شماره ۸۷- پاییز ۱۴۰۳
صص: ۱۱۱ - ۱۴۸
تاریخ دریافت: ۱۴۰۴/۰۵/۱۲ تاریخ پذیرش:۱۴۰۴/۰۷/۰۵

Amniat Pajouhi: Security Research Quarterly
Vol.23, No.87,Autumn 2024
P-P: 111 - 148

تشخیص تهدیدت سایبری سامانه های سایبرفیزیک با استفاده از هوش مصنوعی

مهدی زارع پور[1]*

چکیده

سامانه‌های سایبرفیزیکی[2] (CPS) با ادغام مؤلفه‌های فیزیکی و سایبری، تحولی اساسی در صنایع مختلف ایجاد کرده‌اند و در سال‌های اخیر با افزایش استفاده از این سامانه‌ها در شبکه‌های پیچیده، در معرض تهدیدات سایبری متنوع‌تر و بیشتری قرار می‌گیرند. این مقاله به بررسی تهدیدات سایبری سامانه‌های سایبرفیزیکی و نقش هوش مصنوعی در تشخیص و کاهش این تهدیدات می‌پردازد. در این پژوهش، ابتدا انواع حملات سایبری متوجه این سامانه‌ها، ازجمله بدافزارها (مانند باج‌افزارها و تروجان‌ها)، حملات انکار سرویس توزیع‌شده (DDoS)، حملات روز صفر (Zero-Day) و تهدیدات داخلی تحلیل شده‌اند. سپس، راهکارهای مبتنی بر هوش مصنوعی برای مقابله با این تهدیدات ارائه شده است. همچنین، چالش‌های عملی پیاده‌سازی این راهکارها، ازجمله نیاز به داده‌های آموزشی معتبر، محدودیت‌های پردازش بلادرنگ و بهینه‌سازی مصرف منابع موردبحث قرارگرفته است. به دلیل ماهیت این سامانه‌ها جامعه آماری این تحقیق ۶ نفر از صاحب‌نظران این حوزه بوده که با مصاحبه و نرم‌افزار MaxQDA داده‌ها مورد تحلیل قرارگرفته است. نتایج نشان می‌دهد که با بهینه‌سازی و ارزیابی تجهیزات و استفاده از هوش مصنوعی امکان تشخیص عملی تهدیدات سایبری بر سامانه‌های سایبرفیزیک وجود دارد. درنهایت، با ارائه نمونه‌های کاربردی و مرور معیارهای ارزیابی (مانند نرخ تشخیص و نرخ خطای مثبت)، این مقاله نشان می‌دهد که ترکیب روش‌های مختلف هوش مصنوعی می‌تواند امنیت سامانه‌های سایبر-فیزیکی را به‌طور چشمگیری بهبود بخشد.

کلمات کلیدی: سامانه سایبرفیزیک، تهدیدات سایبری، بدافزارهای، هوش مصنوعی، یادگیری ماشین، تشخیص ناهنجاری

---

۱. استادیار دانشکده علوم و فنون فارابی Mehdizare@aut.ac.ir

2. Cyber Physics System

مقدمه

فنّاوری‌های اخیر مانند رایانش ابری، سامانه‌های سایبر-فیزیکی، هوش مصنوعی، رباتیک و زنجیره بلوکی با ادغام پردازش داده‌ها، ارتباطات، ذخیره‌سازی و روش‌های فیزیکی، در حال دگرگونی تمام عرصه‌های دنیا هستند (Alowaidi et al., 2023, p. 5). اصطلاح سامانه‌های سایبر-فیزیکی به اتصال و هماهنگی تنگاتنگ بین منابع محاسباتی و فیزیکی اشاره دارد؛ به‌عبارت‌دیگر، این سامانه‌ها شامل موجودیت‌های هوشمندی مانند خودروهای خودران، ربات‌ها، ساختمان‌ها، شبکه‌های برق، تولیدات صنعتی و دستگاه‌های پوشیدنی هستند که در فضای سایبر باهم در ارتباط هستند (Baheti & Gill, 2011, pp. 3-4). با توجه به تعریفی که بیان شد می‌توان گفت که جهان و فرآیندهای آن، شامل نهادهای محاسباتی به‌هم‌پیوسته‌ای است که به‌عنوان یک سامانه سایبرفیزیک با یکدیگر کار می‌کنند.

اگرچه سامانه‌های سایبرفیزیکی ارتباط نزدیکی با اینترنت اشیا دارند، اما متفاوت بوده و درعین‌حال به دلیل ارتباط منحصربه‌فردشان با دنیای واقعی یکدیگر را تکمیل می‌کنند. می‌توان بیان کرد سایبرفیزیک در اصل مجموعه‌ای از اینترنت اشیا است که درهم‌تنیده شده‌اند. نکته مهمی که در اینجا وجود دارد این است که حتی در سامانه‌های سایبرفیزیک نیز حمله‌های سایبری می‌توانند منجر به خرابی یا فروپاشی سامانه‌های فیزیکی و واقعی شوند (Yaacoub et al., 2020a, pp. 1-5).

ازطرفی سامانه‌های سایبرفیزیک با بهره‌گیری از حسگرها و محرک‌ها، پیوندهای هوشمند بین آن‌ها و مدل‌های تجاری نوین، فرصت‌هایی برای توسعه راه‌حل‌های پیشرفته فنّاوری اطلاعات و ارتباطات فراهم و منابعی برای ارتقای ساختارهای رایانه‌ای (مانند محیط‌های هوشمند و اینترنت اشیا) ایجاد می‌کنند که حوزه‌های جذابی برای کاربردهای جدید هوش مصنوعی محسوب می‌شوند (Carreras Guzman et al., 2020, p. 3).

۱. بیان مسئله

سامانه‌های سایبرفیزیک از طریق فنّاوری اطلاعات و ارتباطات قابلیت‌های زیادی در رایانش، ذخیره‌سازی و شبکه‌های رایانه‌ای و ارتباطی ارائه می‌دهند که می‌توان آن‌ها را با استفاده از سامانه‌های امنیتی پیشگیری از نفوذ[1] (متناسب با نیازهای طیف گسترده‌ای

1. IPSSs

از صنایع و سازمان‌ها) سفارشی کرد. کاهش هزینه‌های فنّاوری اطلاعات و ارتباطات به کسب‌وکارهای کوچک و متوسط اجازه می‌دهد با خرید نرم‌افزارها یا سخت‌افزارهای موردنیاز، عملکردی بالا داشته باشند (Fitzgerald et al., 2019, pp. 1-3). بااین‌حال، حتی در سامانه‌های سایبرفیزیک نیز حملات سایبری ممکن است اختلال ایجاد کنند؛ به‌عبارت‌دیگر، حسگرها، محرک‌ها و فرآیندهای سامانه اغلب هدف حملات سایبری یا نقص‌هایی هستند و چون‌که در یک سامانه واحد ادغام‌شده‌اند همه بخش‌ها من‌جمله سامانه‌های سایبرفیزیک را دربر می‌گیرند.

نمونه بارز یک حمله مخرب، حمله به شبکه برق اوکراین بود. شبکه برق به‌عنوان یک سامانه سایبرفیزیک، شامل نیروگاه‌ها، ایستگاه‌های انتقال و توزیع، مصرف‌کنندگان، مراکز کنترل و شبکه‌های ارتباطی است. در این سامانه، حسگرها به نظارت بر اجزای مختلف پرداخته و شبکه‌های ارتباطی آن‌ها را به یکدیگر متصل می‌کنند تا سلامت عملکرد سامانه تضمین شود.

در سال ۲۰۱۵، سامانه برق اوکراین به دلیل وجود حجم زیادی از اطلاعات منتشرشده در دسترس عموم، هدف مناسبی برای مهاجمان بود. حمله با ارسال ایمیل فیشینگ آغاز شد که بدافزار BlackEnergy را در شبکه پخش کرد. این بدافزار به مهاجمان امکان دسترسی به داده‌های محرمانه و اطلاعات حیاتی سامانه را داد. با استفاده از این دسترسی، مهاجمان توانستند از راه دور به مراکز کنترل نفوذ کرده و پست‌های برق را غیرفعال کنند.

در مرحله بعد، بخش دیگری از بدافزار فعال شد که با تخریب فایل‌های حیاتی، امکان راه‌اندازی مجدد سامانه را مختل کرد. هم‌زمان، با اجرای حمله محرومیت از سرویس (DoS) علیه مراکز تماس، امکان دریافت اطلاعات به‌روزشده درباره قطعی برق از بین رفت. این حمله منجر به قطعی برق برای حدود ۲۲۵,۰۰۰ مصرف‌کننده به مدت ۱ تا ۶ ساعت شد (W. Duo et al., 2022, p. 2).

یکی دیگر از حملات به سامانه‌های سایبرفیزیک حمله استاکس‌نت[1] که به‌منظور تخریب کنترل‌کننده‌های هسته‌ای تأسیسات صنعتی طراحی شده بود، یکی از پیچیده‌ترین و هدفمندترین حملات سایبری تاریخ محسوب می‌شود. این بدافزار پیشرفته، به‌طور خاص

1. Stuxnet

سامانه‌های کنترل صنعتی (اسکادا) شرکت‌های زیمنس را هدف قرارداد و با آلوده‌کردن برنامه‌نویسی منطقی (PLC)ها، باعث ایجاد اختلال در سانتریفیوژهای غنی‌سازی اورانیوم در تأسیسات هسته‌ای نطنز ایران شد. استاکس‌نت از چهار آسیب‌پذیری صفر روزه بهره برد و از طریق حافظه‌های USB آلوده منتشر شد. این حمله نشان‌داد که چگونه یک حمله سایبری می‌تواند مستقیماً زیرساخت‌های فیزیکی حیاتی را هدف قرارداده و خسارات ملموس ایجاد کند. حملات سایبری مهم دیگری در جدول ۱ آورده شده است که هر یک خسارات قابل‌توجهی به صنعت جهانی وارد کرده است. با توجه به موارد بیان‌شده، در این مقاله سعی شده است که تهدیدات سایبری سامانه‌های سایبرفیزیک معرفی کرده و این تهدیدات را با استفاده از هوش مصنوعی تشخیص داده شود.

جدول ۱. حملات سایبری مهم از سال ۲۰۱۰ تاکنون(W. Duo et al., 2022, p. 2; Zang et al., 2025, p. 3)

ردیف	سال	کشور/صنعت	جزئیات
۱	۲۰۱۰	ایران	حمله استاکس‌نت که کنترل‌کننده‌های مرکزی صنایع را نابود کرد.
۲	۲۰۱۵	اوکراین	حمله BlackEnergy به شبکه برق که منجر به قطعی گسترده برق شد.
۳	۲۰۱۷	روسیه، اوکراین، هند و چین	حمله واناکرای (WannaCry) با هدف رمزگذاری داده‌ها و درخواست باج.
۴	۲۰۲۰	بیمارستان دانشگاه برنو، جمهوری چک	حمله‌ای سایبری که شبکه فنّاوری اطلاعات یک بیمارستان در جمهوری چک را تعطیل کرد.
۵	۲۰۲۰	دپارتمان ایالات‌متحده، سرویس‌های سلامت	حمله نامشخص به سرورها
۶	۲۰۲۱	خط لوله نفت Colonial	حمله باج‌افزاری به خط لوله سوخت ایالات‌متحده که منجر به تعطیلی یک شبکه حیاتی سوخت شد.
۷	۲۰۲۲	ایستگاه‌های فرعی فشارقوی در اوکراین	قبل از ایجاد حادثه واقعی متوقف شد.
۸	۲۰۲۳	ایتالیا	ازکارافتادن سرویس وب

ضرورت و اهمیت

۱-۱ اهمیت

سامانه‌های سایبرفیزیک به‌سرعت در حال نفوذ در صنایع، سازمان‌ها هستند و به‌طوری‌که در سال‌های اخیر زندگی بشر بدون این سامانه‌ها غیرقابل‌تصور است. همان‌طور که در قبل بیان شد این سامانه‌ها در مواجهه به حملات مختلف و متنوع سایبری هستند. نتایج این مقاله نشان می‌دهد که با تشخیص تهدیدات سایبری سامانه‌های سایبرفیزیک می‌توان به نتایج زیر رسید:

- افزایش قابلیت اطمینان و ایمنی سامانه‌هایی مانند شبکه‌های برق، حمل‌ونقل و درمان.
- شناسایی تهدیدات نوظهور و پیچیده که توسط روش‌های سنتی قابل‌تشخیص نیستند.
- کاهش زمان پاسخگویی به حملات از طریق تحلیل بلادرنگ داده‌ها.
- پیش‌بینی و جلوگیری از حملات قبل از وقوع با استفاده از قابلیت‌های پیش‌بینانه هوش مصنوعی.
- حفاظت از زیرساخت‌های حیاتی در برابر حملات سایبری که می‌توانند پیامدهای فیزیکی فاجعه‌بار داشته باشند.
- کاهش خسارات مالی و عملیاتی ناشی از توقف یا اختلال در خدمات.
- توانایی تحلیل حجم انبوه داده‌های تولیدشده توسط سامانه‌های سایبرفیزیکی .
- خودکارسازی فرآیند تشخیص و پاسخ به تهدیدات که وابستگی به نیروی انسانی را کاهش می‌دهد.
- افزایش دقت تشخیص و کاهش تعداد هشدارهای اشتباه[1].
- کمک به تدوین استانداردها و سیاست‌های امنیتی قوی‌تر برای محافظت از فضای سایبری ملی.

1. False Positives

۱-۲ ضرورت

همان‌گونه که در جدول ۱ نشان‌داده شده است، به دلیل حجم زیاد اطلاعات تولیدی سامانه‌های سایبرفیزیک درصورتی‌که در زمان درست و به‌موقع تهدیدات سایبری علیه این سامانه‌ها تشخیص داده نشود ضربات سنگینی به زیرساخت‌هایی از قبیل شبکه برق، حمل‌ونقل وارد می‌شود. در ادامه مواردی از قبیل موارد که ضرورت اجرای این پژوهش را بیان می‌کند، ارائه شده است:

- کاهش قابلیت اطمینان و ایمنی سامانه‌هایی مانند شبکه‌های برق، حمل‌ونقل و درمان.
- افزایش خسارات مالی و عملیاتی ناشی از توقف یا اختلال در خدمات.
- ضعف در برابر تهدیدات نوظهور و پیچیده
- عدم حفاظت از زیرساخت‌های حیاتی در برابر حملات سایبری که می‌توانند پیامدهای فیزیکی فاجعه‌بار داشته باشند.
- عدم توانایی تحلیل حجم انبوه داده‌های تولیدشده توسط سامانه‌های سایبرفیزیکی .

۲. اهداف و سؤالات پژوهش

الف. هدف اصلی

تشخیص تهدیدات سایبری سامانه‌های سایبرفیزیک با استفاده از هوش مصنوعی

ب. اهداف فرعی

- تشخیص تهدیدات سایبری سامانه‌های سایبرفیزیک با استفاده از روش مبتنی بر امضا
- تشخیص تهدیدات سایبری سامانه‌های سایبرفیزیک با استفاده از روش مبتنی بر رفتار
- تشخیص تهدیدات سایبری سامانه‌های سایبرفیزیک با استفاده از یادگیری ماشین

ج. سؤال اصلی

روش‌های تشخیص تهدیدات سایبری سامانه‌های سایبرفیزیک با استفاده از هوش مصنوعی کدامند؟

ب. سؤالات فرعی

- روش‌های تشخیص تهدیدات سایبری سامانه‌های سایبرفیزیک با استفاده از روش مبتنی بر امضا کدامند؟
- روش‌های تشخیص تهدیدات سایبری سامانه‌های سایبرفیزیک با استفاده از روش مبتنی بر رفتار کدامند؟
- روش‌های تشخیص تهدیدات سایبری سامانه‌های سایبرفیزیک با استفاده از یادگیری ماشین کدامند؟

به دلیل ماهیت اکتشافی بودن این پژوهش؛ لذا فرضیه‌ای برای آن متصور نیست.

۳. روش تحقیق و تحلیل داده‌ها

این پژوهش در زمره پژوهش‌های مبتنی بر فنّاوری‌های پیشرفته است بنابراین از نوع تحقیق اکتشافی و از منظر هدف کاربردی و ازنظر ماهیت توسعه‌ای است.

به‌طورکلی این پژوهش با هدف تشخیص تهدیدات سایبری در سامانه‌های سایبرفیزیک انجام می‌پذیرد؛ بنابراین به‌منظور رسیدن به این هدف، از رویکرد کیفی بهره گرفته شده است تا از نظرات نخبگان و خبرگان در این حوزه استفاده شود. داده‌های کیفی حاصل از مصاحبه‌ها و جلسات دلفی از طریق تحلیل محتوا برای شناسایی و اولویت‌بندی انواع روش‌های تشخیص و روش‌های مورداستفاده دز هوش مصنوعی موردبررسی قرارگرفته شده است.

جامعه آماری در این پژوهش شامل متخصصان، کارشناسان و تصمیم‌گیرانی هستند که به‌طور مستقیم یا غیرمستقیم با موضوع سامانه‌های سایبرفیزیک سروکار دارند. ویژگی‌هایی این جامعه آماری (خبرگان) مواردی از قبیل: تخصص و دانش، تجربه کاری مرتبط، دیدگاه حل مسئله، تنوع دیدگاه و دسترسی‌پذیری است که با توجه به این موارد تعداد ۶ نفر از صاحب‌نظران حوزه سامانه‌های سایبرفیزیک که آشنا به امنیت، تهدید و هوش مصنوعی هستند به‌عنوان حجم جامعه آماری این تحقیق هستند.

۵-۱ روش و ابزار گردآوری

روش گردآوری اطلاعات به دودسته اسنادی (کتابخانه‌ای و اینترنتی) و میدانی (مصاحبه) تقسیم می‌شود. در خصوص اطلاعات مربوط به ادبیات تحقیق از روش‌های کتابخانه‌ای

و اینترنتی و جهت تکمیل، تحلیل و تأیید اطلاعات از روش میدانی (مصاحبه) استفاده شده است.

برای رسیدن به هدف این پژوهش انتخاب ابزار مناسب برای گردآوری داده به ماهیت حساس، پیچیده موضوع بستگی دارد که از ابزارهایی از قبیل منابع اطلاعاتی باز، پایگاه داده علمی و تحلیلی، روش دلفی و مصاحبه‌های خبرگان استفاده شده است.

۵-۲ شیوه تجزیه‌وتحلیل داده‌ها

تجزیه‌وتحلیل داده‌ها در این پژوهش مرحله‌ای بعد از گردآوری داده‌ها است. تحلیل داده‌ها باید به شناسایی روش‌های تشخیص، روش‌های مورداستفاده در هوش مصنوعی مرتبط با سامانه‌های سایبرفیزیک منجر شود و لذا با استفاده از تحلیل محتوای کیفی با استفاده از نرم‌افزار MaxQDA این تحلیل انجام شده است.

۴. مبانی نظری

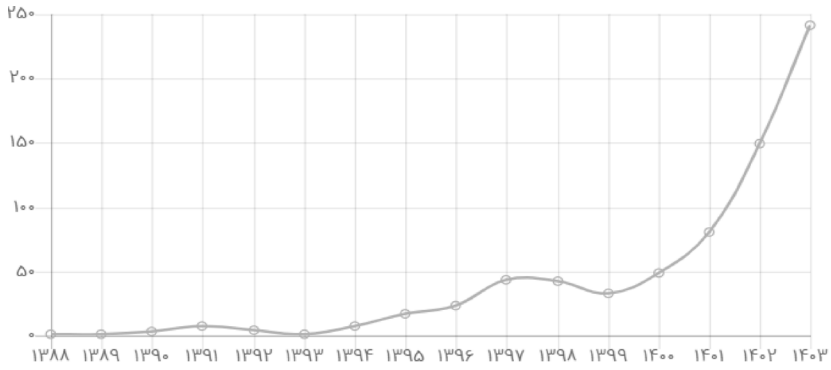
در سال‌های اخیر، هم‌راستا با پیشرفت فنّاوری، تهدیدات سایبری نیز به‌سرعت در حال افزایش و تغییر است و به دلیل اهمیت زیاد این حوزه، موردتحقیق و پژوهش محققان بسیار قرارگرفته است به‌طوری‌که در کشورمان روند تحقیقات در حوزه تهدیدات سایبری تا سال ۱۴۰۳ در شکل ۱ نشان‌داده شده است. در ادامه به برخی از این تحقیقات پرداخته می‌شود.

روند افزایش تهدیدات سایبری طوری شده است که امروزه این تهدیدات به‌جای تهدیدات کلاسیک نظامی موردتوجه پژوهش‌های امنیتی است و در این میان تأثیرگذاری آن بر امنیت اقتصادی جوامع تحت نفوذ فنّاوری‌های نوین دیجیتالی عرصه جدیدی را برای مطالعه این تهدیدات ایجاد کرده است. ورود و نفوذ این فنّاوری‌های نوین دیجیتال در تمامی سطوح حکمرانی ایران، موجب بروز تهدیدات و حملاتی از جنس سایبری شده است. این امر با توجه جنس اقتصاد ایران توانسته تهدیداتی را با خود برای امنیت اقتصادی ایران به همراه داشته باشد (لک، ۱۴۰۰:. ۳۶).

دسته‌ای دیگر از تهدیدات سایبری، تهدیدات پایدار پیشرفته[1] به‌عنوان یک مفهوم جدید در جنگ سایبری نگرانی‌های زیادی را ایجاد کرده است. حملات سایبری مبتنی بر APT

1. APT: Advanced Persistent Threat

معمولاً مخفیانه، گام‌به‌گام، آهسته و طولانی‌مدت هستند. این حملات برنامه‌ریزی‌شده و بر اساس مجموعه‌ای از آسیب‌پذیری‌های متنوع روز صفر عمل می‌کنند. درنتیجه، این حملات تا حد ممکن متنوع و پویا رفتار می‌کنند؛ ازاین‌رو هشدارهای ایجادشده برای این حملات به‌طورمعمول زیر حد آستانه تشخیص حملات متداول هستند؛ بنابراین، رویکردهای فعلی عمدتاً قادر به شناسایی یا تجزیه‌وتحلیل رفتار این دسته از حملات نیستند (خسروی، ۱۳۹۹: ۱۳).



شکل ۱ نمایش تعداد تحقیقات در مورد تهدیدات سایبری[1]

۱-۱ انواع بدافزارها

بدافزار به برنامه‌های مخربی گفته می‌شود که عمداً در یک سامانه نصب می‌شوند تا قابلیت اطمینان، محرمانگی یا دسترس‌پذیری داده‌ها را مختل کنند و یا اعمالی غیر از هدف کاربر سامانه انجام دهد. این برنامه‌های مخرب که به‌صورت پنهانی اجرا می‌شوند، می‌توانند بر داده‌های شخصی، برنامه‌های کاربردی و حتی سامانه عامل تأثیر بگذارند. اجرای پنهان و بدون اطلاع کاربر از ویژگی‌های همه بدافزارها است که هدف اصلی آن دست‌کاری در سه اصل اساسی امنیت اطلاعات یعنی یکپارچگی داده‌ها[2]، محرمانگی[3]، دسترس‌پذیری[4] است. دست‌کاری این سال منجر به اتفاقاتی از قبیل ایجاد اختلال گسترده در سامانه‌ها، نیاز به صرف منابع و تلاش قابل‌توجه برای مقابله و ... می‌شود و

1. Irandoc.ac.ir
2. Reliability
3. Confidentiality
4. Availability

باعث تبدیل‌شدن به یکی از مهم‌ترین تهدیدات خارجی برای سامانه‌های رایانه‌ای می‌گردد.

چالش‌های مقابله با بدافزارهای را می‌توان به‌صورت زیر تقسیم‌بندی نمود:

- پیچیدگی روزافزون بدافزارها
- نیاز به تخصیص منابع انسانی و مالی قابل‌توجه در سازمان‌ها
- ضرورت به‌روزرسانی مستمر سامانه‌های امنیتی

با توجه به اینکه توسعه و گسترش بدافزارها به یکی از نگرانی‌های اصلی متخصصان امنیت سایبری تبدیل شده است؛ چراکه این تهدیدات می‌توانند خسارات مالی و اطلاعاتی جبران‌ناپذیری به افراد و سازمان‌ها وارد کنند. به‌طور عمومی می‌توان تهدیدات فضای سایبر را به دسته کلی بدافزارها تقسیم‌بندی نمود که رایج‌ترین انواع بدافزارها را می‌توان به‌صورت زیر دسته‌بندی کرد (Erbschloe, 2004, p. 7):

ویروس رایانه‌ای

این بدافزار پس از اجرا، با تغییر برنامه‌های دیگر و واردکردن کد خود، تکثیر می‌شود. ویروس‌های رایانه‌ای عموماً نیاز به یک برنامه میزبان دارند تا کد خود را در آن بنویسند. پس از اجرای کد، ویروس نوشته‌شده ابتدا اجرا می‌شود و باعث آلودگی و خسارت می‌گردد. در مقابل، کرم رایانه‌ای نیازی به برنامه میزبان ندارد (زیرا یک کد خودگردان یا بخشی مستقل از برنامه است)، بنابراین محدودیتی توسط برنامه میزبان ندارد و می‌تواند به‌صورت مستقل و تهاجمی اقدامات مخرب را انجام دهد.

نویسندگان ویروس‌ها از فریب‌های مهندسی اجتماعی و سوءاستفاده از ضعف‌های دانش امنیت سایبری برای آلوده‌سازی سامانه‌ها و گسترش مشکل استفاده می‌کنند. ویروس‌ها از راه‌کارهای پیچیده ضدتشخیص/استتار برای فرار از نرم‌افزارهای آنتی‌ویروس بهره می‌برند. انگیزه‌های ساخت ویروس ممکن است شامل سودجویی (مثل باج‌افزارها)، انتقال پیام سیاسی، شوخی شخصی، اثبات آسیب‌پذیری نرم‌افزاری، خرابکاری، ایجاد حمله DoS، یا حتی پژوهش در مورد نگرانی‌های امنیتی، الگوریتم‌های تکاملی و زندگی مصنوعی باشد. ویروس‌ها سالانه میلیاردها دلار خسارت اقتصادی وارد می‌کنند. در

پاسخ، صنعت آنتی‌ویروس شکل گرفته است که نرم‌افزارهای محافظتی را به‌صورت تجاری یا رایگان در اختیار کاربران سامانه‌های عامل قرار می‌دهد.

برخی ویروس‌ها ممکن است صرفاً فایل‌های مشکوک را علامت‌گذاری کنند. روش قدیمی اما فشرده برای تشخیص، استفاده از عملیات ریاضی مثل جمع، تفریق و عملیات بولی مانند (XOR) است که در آن هر بایت ویروس با یک ثابت پردازش می‌شود؛ بنابراین، عملیات XORتنها برای رمزگشایی تکرار می‌شود. اگر کدی بتواند خود را تغییر دهد (خودتغییرپذیر باشد)، بخش‌های رمزنگاری/رمزگشایی ممکن است به‌عنوان امضای ویروس در تعاریف آنتی‌ویروس استفاده شوند.

روش‌های ساده‌تر از کلید استفاده نمی‌کردند مثلاً عملیات افزایش/کاهش، نفی ریاضی (NOT)، منطقی یا چرخش بیتی. برخی ویروس‌ها موسوم به ویروس‌های چندریختی[1]، رمزنگاری را درون فایل اجرایی انجام می‌دهند. این ویروس‌ها در شرایط خاصی (مثل خاموش بودن اسکنر آنتی‌ویروس برای به‌روزرسانی یا راه‌اندازی مجدد سامانه) رمزگذاری می‌شوند. ویروس‌های چندریختی اولین تهدید جدی برای آنتی‌ویروس‌ها بودند: آن‌ها فایل‌ها را با نسخه رمزگذاری‌شده خود آلوده می‌کنند و مانند ویروس‌های معمولی توسط یک بلوک رمزگشایی، کد می‌شوند؛ اما در هر آلودگی، ماژول رمزگشایی را تغییر می‌دهند؛ بنابراین، یک ویروس چندریختیِ حرفه‌ای هیچ بخش یکسانی بین آلودگی‌های مختلف ندارد و تشخیص مستقیم آن از طریق امضا را دشوار می‌کند. آنتی‌ویروس‌ها ممکن است با شبیه‌سازی (امولاتور) یا تحلیل الگوی آماری بدنهٔ رمزگذاری‌شده ویروس، آن را شناسایی کنند.

ویروس‌های چندریختی موتور چندریختی‌ساز[2] در بدنهٔ رمزگذاری‌شده خود دارند. برخی ویروس‌ها از کدهای چندریختی استفاده می‌کنند که نرخ تغییر آن‌ها را محدود می‌سازد (مثلاً تغییرات بسیار کند یا توقف پس از آلودگی فایل‌های حاوی کپی ویروس). این کُندی، جمع‌آوری نمونه‌های نماینده ویروس را برای محققان امنیتی سخت می‌کند، زیرا فایل‌های طعمه در یک اجرا معمولاً نمونه‌های یکسان یا مشابهی تولید می‌کنند. این

1. Polymorphic
2. Mutation Engine

روش، تشخیص توسط آنتی‌ویروس‌ها را غیرقابل‌اعتماد کرده و درنهایت برخی نمونه‌های از ویروس امکان فرار دارند.

برخی ویروس‌ها پس از هر آلودگی، کد خود را کاملاً بازنویسی می‌کنند که به کدهای دگردیسی‌پذیر[1] معروفند. این کدها از تشخیص توسط شبیه‌سازی جلوگیری می‌کنند. این ویروس‌ها نیاز به یک موتور دگردیسی دارند و معمولاً حجیم و پیچیده هستند.

کرم رایانه‌ای

این برنامه مخرب مستقل، با تکثیر خود، سایر رایانه‌ها را آلوده می‌کند. کرم‌ها معمولاً از طریق شبکه‌های رایانه‌ای منتشر می‌شوند و با سوءاستفاده از نقاط ضعف امنیتی در سخت‌افزار هدف، به آن دسترسی پیدا می‌کنند. سپس از این میزبان برای اسکن و آلوده‌کردن تجهیزات دیگر استفاده می‌کنند. هنگامی‌که دستگاه‌های جدید توسط کرم تسخیر می‌شوند، به‌صورت مداوم به رصد و آلوده‌سازی رایانه‌های دیگر ادامه می‌دهند و این چرخه تکرار می‌شود.

کرم‌ها از روش‌های بازگشتی برای انتشار کپی‌های خود (بدون نیاز به برنامه میزبان) و توزیع مجدد استفاده می‌کنند و با بهره‌گیری از مزایای رشد نمایی، به‌سرعت کنترل رایانه‌های بیشتری را در دست گرفته و آن‌ها را آلوده می‌کنند. کرم‌ها با ویروس‌ها تفاوت‌هایی دارند که می‌توان به‌صورت زیر خلاصه نمود:

- کرم‌ها تقریباً همیشه باعث اختلال در شبکه می‌شوند (حتی اگر صرفاً پهنای باند را مصرف کنند)، درحالی‌که ویروس‌ها معمولاً فایل‌های رایانه هدف را تخریب یا تغییر می‌دهند.
- بسیاری از کرم‌ها بدون ایجاد تغییر در سامانه‌ها، صرفاً منتشر می‌شوند. نمونه‌هایی مانند **کرم موریس**[2] و **مایدوم**[3] نشان‌دادند که حتی کرم‌های فاقد بار مخرب[4] نیز می‌توانند با ایجاد ترافیک انبوه شبکه و اثرات غیرمنتظره، اختلالات گسترده‌ای به وجود آورند.

1. Metamorphic
2. Morris
3. Mydoom
4. Payload-free

مهندسی اجتماعی

مهندسی اجتماعی بهره‌برداری روان‌شناختی از افراد برای وادارکردن آن‌ها به انجام اقدامات خاص یا افشای اطلاعات محرمانه به‌منظور کلاه‌برداری یا دسترسی غیرمجاز به سامانه‌ها است. یک مهاجم مهندسی اجتماعی با کلاه‌برداران سنتی تفاوت دارد، زیرا مهندسی اجتماعی معمولاً شامل مراحل متعدد در یک الگوی کلاه‌برداری پیچیده‌تر است. این روش همچنین به‌عنوان «هر عملی که فردی را ترغیب به انجام اقدامی برخلاف منافع خود کند» توصیف می‌شود. به‌طور مثال: مهاجمی با جعل هویت، از بخش پشتیبانی یک شرکت درخواست اطلاعات می‌کند و با وانمود کردن به اینکه کاربری دیگر است، تقاضای بازنشانی رمز عبور می‌نماید. اگر کارمند پشتیبانی این درخواست را بپذیرد، مهاجم به‌راحتی به‌حساب کاربری دسترسی کامل پیدا خواهد کرد. چرخه حیات مهندسی اجتماعی به‌صورت زیر است:

الف) جمع‌آوری اطلاعات: اولین و مهم‌ترین مرحله در چرخه است که به صبر و دقت زیادی برای بررسی عادات قربانی نیاز دارد. در این مرحله، اطلاعاتی درباره علایق و داده‌های شخصی قربانی جمع‌آوری می‌شود که میزان موفقیت کل عملیات را تعیین می‌کند.

ب) تعامل با قربانی: پس از جمع‌آوری اطلاعات لازم، مهاجم به‌آرامی با قربانی وارد گفتگو می‌شود به‌گونه‌ای که قربانی باور کند این تعامل کاملاً قانونی و بی‌خطر است.

ج) حمله: این مرحله معمولاً پس از دوره‌ای طولانی از تعامل با قربانی انجام می‌شود. در این فاز، مهاجم به اطلاعات یا منابع موردنظر دسترسی پیداکرده و از آن‌ها سوءاستفاده می‌کند.

د) پایان تعامل: در این مرحله نهایی، مهاجم به‌تدریج ارتباط خود را با قربانی قطع می‌کند، بدون اینکه هیچ شک و شبهه‌ای ایجاد کند. بدین‌ترتیب هدف محقق شده و قربانی معمولاً متوجه نمی‌شود که موردحمله قرارگرفته است.

باج‌افزار

این نوع پیشرفته از بدافزارها با استفاده از تکنیک‌های رمزنگاری، قربانی را تحت‌فشار قرار می‌دهد تا برای بازگرداندن دسترسی به داده‌هایش باج پرداخت کند. در صورت عدم

پرداخت، مهاجمان ممکن است داده‌ها را منتشر کرده یا دسترسی به آن‌ها را برای همیشه مسدود نمایند.

سطح‌بندی باج‌افزارها

- **انواع ساده**
  - فقط دسترسی به سامانه را محدود می‌کنند.
  - معمولاً به فایل‌ها آسیب نمی‌زنند.
- **انواع پیشرفته**
  - از تکنیک‌های رمزنگاری پیچیده استفاده می‌کنند.
  - فایل‌ها را کاملاً دسترس‌ناپذیر می‌کنند.
  - نیازمند کلید رمزگشایی اختصاصی هستند.

سازوکار عمل باج‌افزارها به‌گونه‌ای است که فایل‌ها را با الگوریتم‌های رمزنگاری قوی کدگذاری می‌کنند که تنها راه بازیابی داده‌ها، پرداخت باج برای دریافت کلید رمزگشایی است و در عملیات حرفه‌ای، بازیابی فایل‌ها بدون کلید رمزگشایی تقریباً غیرممکن است. در باج‌افزارها چالش‌های امنیتی نیز امکان دارد به وجود آید که می‌توان به مواردی از قبیل استفاده مهاجمان از ارزهای دیجیتال غیرقابل ردیابی، دشواری شناسایی و پیگرد قانونی مجرمان و افزایش پیچیدگی حملات در نمونه‌های جدید نام برد. برای ایمنی از این نوع بدافزار بایستی از داده‌های مهم به‌طور منظم نسخه پشتیبان گرفت و نرم‌افزارهای امنیتی نصب شود و مداوم به‌روزرسانی گردد. دسترسی کاربران به حداقل سطح موردنیاز محدود شود و در خصوص باج‌افزارها به آن‌ها آموزش‌های لازم داده شود. این نوع حمله سایبری در سال‌های اخیر به یکی از تهدیدات اصلی برای سازمان‌ها و افراد تبدیل شده است و مقابله با آن نیازمند رویکردی چندلایه شامل پیشگیری، تشخیص و واکنش سریع است.

۲-۱ حملات سایبری و تهدیدات امنیتی در سامانه‌های سایبرفیزیکی

تهدیدات سایبری که در بخش قبل به‌عنوان بدافزار معرفی‌شده‌اند، می‌توانند علیه سامانه‌های سایبرفیزیک مورداستفاده قرار گیرند و در اصل به این سامانه‌ها حمله نمایند. لازم است در ادامه این تحقیق حملاتی که علیه سامانه‌های سایبرفیزیک متصور است معرفی شود (Szor, 2005, pp. 8–9).

- **حملات باج‌افزاری و استفاده از ارزهای دیجیتال**

حمله باج‌افزار علیه این‌گونه سامانه‌ها بسیار مورداستفاده قرارمی‌گیرد و استفاده از ارزهای دیجیتال، به‌ویژه انواعی که ردیابی آن‌ها دشوار است، در قالب باج‌افزاری، پیگیری و تعقیب قانونی افراد مسئول را پیچیده می‌کند. حملات تخریب داده‌ها معمولاً شامل یک تروجان هستند که به شکل یک فایل قانونی استتار شده و قربانی را فریب می‌دهد تا آن را ناخواسته دانلود یا باز کند، اغلب از طریق پیوست ایمیل. بااین‌حال، یک نمونه بارز، باج‌افزار WannaCry بود که می‌توانست به‌صورت خودکار بین دستگاه‌ها بدون نیاز به تعامل کاربر گسترش یابد.

- **حمله فیشینگ**

این روش از ایمیل‌ها یا وب‌سایت‌های فریبنده برای سرقت داده‌های حساس مانند جزئیات حساب بانکی استفاده می‌کند. مجرم خود را به‌عنوان یک شرکت یا فرد معتبر جا می‌زند. حملات فیشینگ شامل ایمیل‌ها، پیام‌های متنی، تماس‌های تلفنی یا وب‌سایت‌های جعلی هستند که کاربران را فریب می‌دهند تا بدافزار دانلود کنند، اطلاعات حساس را به اشتراک بگذارند (مانند اطلاعات هویتی، شماره کارت اعتباری/حساب بانکی، اطلاعات ورود) یا اقداماتی را انجام دهند که آن‌ها را در معرض جرائم سایبری قرار می‌دهد. حملات فیشینگ موفق می‌توانند منجر به کلاه‌برداری با کارت اعتباری، سرقت هویت، شیوع بدافزارهای تخریب‌کننده داده‌ها، نشت داده‌ها و زیان‌های مالی بزرگ شخصی یا شرکتی شوند. متداول‌ترین نوع مهندسی اجتماعی، حمله فیشینگ است که قربانیان را فریب می‌دهد، تحت‌فشار قرار می‌دهد یا دست‌کاری می‌کند تا پول یا اطلاعات را به افراد نادرست تحویل دهند. موفقیت حملات مهندسی اجتماعی ناشی از خطاهای انسانی و فشار است. مهاجم معمولاً خود را به‌عنوان همکار، مدیر یا کسب‌وکاری که قربانی به آن اعتماد دارد، جا می‌زند و حس فوریت ایجاد می‌کند تا قربانی سریع عمل کند که این روش ارزان‌تر و آسان‌تر از هک کردن یک رایانه یا شبکه است. بیشتر حملات سایبری از طریق ایمیل‌های فیشینگ به افراد و سازمان‌ها منتشر می‌شوند. «فیشینگ هدفمند» نوعی حمله فیشینگ است که افراد خاص را هدف قرار می‌دهد و شامل علایق آن‌ها می‌شود، مانند رویدادهای شخصی جاری یا مسائل مالی.

- **حمله منع سرویس توزیع‌شده**

مهاجم با ارسال حجم عظیمی از ترافیک به یک سرور، دسترسی کاربران اینترنت به خدمات و سایت‌های آنلاین را مسدود می‌کند و باعث توقف ترافیک عادی سایت که به‌عنوان بسته‌های معتبر شناخته می‌شود، می‌گردد. مهاجمان این کار را با هدایت ترافیکی بیش‌ازحد توان قربانی انجام می‌دهند که باعث ازکارافتادن سرور و عدم توانایی آن در ارائه خدمات به کاربران عادی می‌شود. اهداف ممکن است شامل وب‌سایت‌ها، ایمیل، بانکداری آنلاین یا سایر خدمات وابسته به شبکه یا دستگاه باشد. یک رایانه یا شبکه تحت حملات «منع سرویس» (DoS) با مشکلاتی مانند کاهش، محدودیت یا توقف دسترسی به منابع سامانه برای کاربران مجاز مواجه می‌شود. حمله DDoS ممکن است چندین سامانه را به‌طور هم‌زمان به خطر بیندازد. مهاجم می‌تواند دستگاه‌های آلوده (زامبی) را به‌صورت تصادفی یا بر اساس توپولوژی انتخاب کند و پس از آلودگی، این نهاد یک واپایشگر/دستورها برای دست‌کاری زامبی‌ها تنظیم می‌کند و رباتی (بات) که یک نرم‌افزار مخرب است را روی دستگاه‌های آسیب‌دیده نصب می‌کند و به مهاجم کنترل زامبی‌ها را می‌دهد. درواقع بات‌نت شبکه‌ای از بات‌ها است که به‌صورت هم‌زمان و یا غیرهم‌زمان فعالیتی خاص را انجام می‌دهند. انواع حملات DoS شامل:

- **بات‌نت**
- این حمله سایبری دستگاه‌های متصل به شبکه زیادی را با بات‌ها آلوده می‌کند و به یک سرور، وب‌سایت شرکت، سایر دستگاه‌ها یا افراد حمله می‌کند. پس از آلودگی، یک بات می‌تواند داده‌های کاربر را جمع‌آوری و سرقت کند، داده‌های سامانه را بخواند و بنویسد، فعالیت کاربر را زیر نظر بگیرد، حملات DDoS انجام دهد، اسپم ارسال کند، حملات brute force را آغاز کند، استخراج رمزنگاری انجام دهد و غیره.

- **حمله حجمی**[1]

- این حمله تمام پهنای باند را مصرف می‌کند، بنابراین کاربران مجاز نمی‌توانند به منابع دسترسی پیدا کنند، زیرا دستگاه‌های شبکه (مانند هاب‌ها و سوئیچ‌ها) با

1. Volumetric

تعداد زیادی بسته درخواست/پاسخ ICMP اشباع می‌شوند. درنتیجه، تمام پهنای باند مصرف می‌شود و سایر کاربران نمی‌توانند به شبکه هدف متصل شوند.

- **سیلاب[1]:SYN**
- مهاجم با آلوده‌کردن چندین زامبی، قربانی را با بسته‌های SYN متعدد بمباران می‌کند. درخواست‌های SYN قربانی را غرق می‌کنند و باعث کاهش شدید عملکرد یا خاموش شدن آن می‌شوند.
- **حملات تکه‌تکه‌سازی[2]**
- این حمله توانایی هدف را در بازسازی بسته‌ها مختل می‌کند. بسته‌های تکه‌تکه شده زیادی به هدف ارسال می‌شوند که توانایی بازسازی آن را مختل می‌کنند و درنتیجه دسترسی کاربران مجاز را مسدود می‌نمایند.

حمله خستگی حالت TCP[3]

- مهاجم با ایجاد و قطع اتصالات TCP ، یک حمله DoS ایجاد می‌کند که جداول پایدار را تحت‌فشار قرار می‌دهد.
- **حملات لایه کاربردی[4]**
- مهاجم از خطاهای برنامه‌نویسی برنامه‌ها برای ایجاد یک حمله DoS سوءاستفاده می‌کند. این کار با ارسال درخواست‌های متعدد به برنامه هدف برای تخلیه منابع انجام می‌شود. درنتیجه، برنامه نمی‌تواند به هیچ مشتری معتبری خدمات ارائه دهد. یک خطای برنامه‌نویسی (مانند سرریز بافر) ممکن است باعث تخصیص حافظه به یک متغیر کوچک‌تر از مقدار درخواستی شود. سپس، نشت حافظه یا خرابی کامل برنامه ممکن است رخ دهد. سایر حملات لایه کاربردی شامل قفل شدن حساب و سیل درخواست‌ها می‌شود.

1. SYN Flooding
2. Fragmentation Attacks
3. TCP-state Exhaustion Attack
4. Application Layer Attacks

- **پاک‌سازی**[1]
- این حمله از طریق به‌روزرسانی‌های جعلی سامانه، آسیب دائمی به سخت‌افزار وارد می‌کند و آن را غیرقابل استفاده می‌نماید. تنها راه‌حل، نصب مجدد سخت‌افزار است.

راه‌کارهای مقابله شامل:

- استفاده از جدیدترین ابزارهای ضدویروس و «ساختار تشخیص نفوذ (IDS)
- انجام تحلیل شبکه برای شناسایی حملاتDoS
- خاموش کردن خدمات شبکه اضافی هدف
- یافتن و خنثی‌سازی واپایشگرها برای محافظت از قربانیان ثانویه
- انجام پروفایل‌سازی فعالیت و فیلتر هوشمند برای حذف ترافیک ناخواسته
- اجرای تحلیل عمیق بسته‌ها
- استفاده از تاکتیک دفاع در عمق
- افزودن متعادل‌کننده‌های بار اضافی برای جذب و کنترل ترافیک
- تصحیح خطاهای برنامه
- استفاده از سازکارهای رمزنگاری قوی

- **اسب تروجان**

این نرم‌افزار مخرب خود را به‌عنوان یک نرم‌افزار معمولی استتار می‌کند تا کاربران را فریب دهد. این اصطلاح از افسانه یونانی اسب تروجان گرفته شده است که منجر به سقوط تروی شد. مهندسی اجتماعی می‌تواند تروجان‌ها را گسترش دهد، به‌عنوان‌مثال، کاربر فریب می‌خورد تا یک پیوست ایمیل که به نظر عادی می‌رسد یا یک تبلیغ جعلی در رسانه‌های اجتماعی را کلیک کند. محموله آن‌ها متفاوت است، اما بسیاری از آن‌ها به‌عنوان یک در پشتی عمل می‌کنند که با یک واپایشگر غیرمجاز برای دسترسی به رایانه ارتباط برقرار می‌نمایند. حملات تخریب داده‌ها برای تروجان‌ها رایج هستند. تروجان‌ها نمی‌توانند مانند ویروس‌ها و کرم‌ها خود را تکثیر یا در فایل‌های دیگر جاسازی کنند (Erbschloe, 2004, p. 2).

1. Plashing

• **حمله مرد میانی**[1]

مهاجمان خود را بین دو طرفی که فکر می‌کنند به‌طور مستقیم و محرمانه در حال ارتباط هستند، قرار می‌دهند و ارتباطات آن‌ها را تغییر می‌دهند. استراق سمع فعال یک حمله مرد میانی است که در آن مهاجم ارتباطات مستقلی بین قربانیان ایجاد می‌کند و پیام‌ها را جعل می‌نماید تا آن‌ها را فریب دهد که فکر کنند از طریق یک لینک امن مستقیماً باهم صحبت می‌کنند، درحالی‌که مهاجم کنترل مکالمه را در دست دارد. مهاجم باید تمام پیام‌های مربوطه بین اهداف را ره‌گیری و تزریق کند. بدون رمزنگاری، یک مهاجم در محدوده نقطه دسترسی Wi-Fi می‌تواند حمله مردمیانی انجام دهد. مهاجم باید هر نقطه پایانی را به‌اندازه کافی خوب جعل کند تا انتظارات طرفین را برآورده نماید تا احراز هویت متقابل در یک حمله مردمیانی را دور بزند. بیشتر پروتکل‌های رمزنگاری بر اساس احراز هویت نقطه پایانی ساخته‌شده‌اند تا از وقوع مردمیانی جلوگیری کنند. مرجع صدور گواهی معتبر می‌تواند یک یا هر دو طرف در یک ارتباط را تأیید کند. سیاست امنیتی شرکت ممکن است شامل افزودن گواهی‌های سفارشی به مرورگرهای وب ایستگاه‌های کاری برای بررسی ترافیک رمزنگاری‌شده باشد؛ بنابراین، یک قفل سبز تضمینی برای تأیید امنیت سرور از راه دور نیست، مگر اینکه سرور/پراکسی کسب‌وکار مسئول بازرسی SSL/TLS باشد. راه‌کارهای ممکن شامل:

الف) **سنجاق کردن کلید عمومی (HPKP) HTTP**: سرور با لیست کردن هش‌های کلید عمومی سنجاق شده در طول اولین اقدام، از وقوع حمله MITM بر روی مرجع صدور گواهی جلوگیری می‌کند. تراکنش‌های بعدی نیاز به احراز هویت سرور با یک یا چند کلید لیست شده دارند. DNSSEC (یک افزونه DNS) از امضاها برای تأیید سوابق DNS استفاده می‌کند و از حملات MITM که مشتریان را به آدرس‌های IP مخرب هدایت می‌کنند، جلوگیری می‌نماید.

ب) **تشخیص دست‌کاری:** یک بررسی تأخیر می‌تواند حمله را در برخی شرایط، مانند محاسبات طولانی در توابع هش، شناسایی کند. برای کشف حملات احتمالی، طرفین درگیر ناهماهنگی در زمان پاسخ را آزمایش می‌کنند. اگر دو طرف معمولاً زمان مشخصی

1. MITMA

برای انجام یک عملیات خاص صرف کنند و انجام آن عملیات زمان غیرعادی ببرد، احتمال دخالت یک‌طرف سوم که تأخیر اضافی ایجاد می‌کند، وجود دارد.

ج) **رمزنگاری کوانتومی (QC):** این روش با استفاده از قضیه عدم کلون‌پذیری، تأیید دست‌کاری برای تراکنش‌ها را فراهم می‌کند. پروتکل‌های QC برخی یا تمام تبادلات را با یک استراتژی احراز هویت امن، مانند طرح Wegman-Carter ، تأیید می‌کنند.

د) **تحلیل پزشکی قانونی (FA):** این روش ترافیک شبکه را از یک حمله مشکوک ضبط می‌کند و می‌تواند برای تعیین وقوع حمله بررسی شود. در صورت تأیید حمله، FA منبع حمله را با استفاده از شواهد محکم برای تحلیل پزشکی قانونی شبکه بر روی یک حمله غیرقابل‌اعتماد، ازجمله موارد زیر انتخاب می‌کند:

- آدرس IP سرور
- نام DNS سرورها
- گواهی X.509 سرورها
- گواهی خودامضا
- گواهی امضاشده توسط مرجع معتبر
- گواهی فسخ‌شده
- گواهی اخیراً تغییریافته
- سایر ذی‌نفعان در اینترنت با همان گواهی

- **جاسوس‌افزار**

این نرم‌افزار حریم خصوصی را نقض می‌کند و به یک نگرانی اصلی برای مؤسسات تبدیل شده است. اگرچه نرم‌افزارهای نقض حریم خصوصی برای چندین سال وجود داشته‌اند، اما امروزه بسیار رایج‌تر شده‌اند و به سامانه‌ها نفوذ می‌کنند تا فعالیت‌های خصوصی را ردیابی کنند و تقلب مالی انجام دهند.

- **تزریق SQL[1]**

تزریق SQL یک تکنیک رایج هک وب است که شامل تزریق کد مخرب در عبارات SQL از طریق صفحات وب می‌شود و ممکن است به یک پایگاه داده آسیب برساند.

1. SQLi

این آسیب‌پذیری امنیتی وب به مهاجم اجازه می‌دهد در پرس‌وجوهای کاربران به یک مخزن داده دخالت کند. این حمله به مهاجم امکان می‌دهد داده‌هایی را که به‌طورمعمول نمی‌تواند بازیابی کند، مشاهده نماید. این اتفاق زمانی رخ می‌دهد که برنامه یک ورودی مخرب را به‌عنوان بخشی از یک عبارت SQL برای پرس‌وجو از یک پایگاه داده بک‌اند بپذیرد. مهاجمان می‌توانند دستورات SQL و کاراکترهای کنترل را وارد کنند تا ساختار پرس‌وجو را تغییر دهند.

- **حمله به اینترنت اشیا**

با دسترسی دستگاه‌های اینترنت اشیا به شبکه، مهاجمان می‌توانند اطلاعات را به‌سمت ابر هدایت کنند و درعین‌حال برای حفظ، حذف یا افشای داده‌ها فشار وارد کنند، مگر اینکه باج پرداخت شود. گاهی اوقات، پرداخت برای یک گروه کافی نیست تا تمام سوابق خود را بازیابی کند و بدافزار تخریب داده‌ها به‌طور خودکار فایل‌ها را حذف می‌کند.

- **تهدید داخلی (InT)**

این خطر امنیت سایبری از درون سازمان نشئت می‌گیرد. این حمله معمولاً زمانی رخ می‌دهد که یک کارمند فعلی یا سابق، پیمانکار، فروشنده یا همکار با اعتبارنامه کاربری معتبر، بتواند به شبکه‌ها، سامانه‌ها و داده‌های مؤسسه دسترسی مضر داشته باشد. می‌توان بیان کرد به دلیل دسترسی‌هایی که کاربران دارند این نوع حمله بیشترین اثر و تخریب را دارد و به‌طورکلی می‌تواند تمامی پروتکل‌های امنیتی وضع‌شده را دور بزند.

- **کریپتوجکینگ**[1]

از زمان ظهور رمزارزها (ارزهای دیجیتال) سرقت آن‌ها به‌عنوان یکی از تهدیدات سایبری به وجود آمد. این حمله شامل ربودن یک دستگاه برای استخراج ارزهای دیجیتال برخلاف میل کاربر از طریق وب‌سایت‌ها یا درزمانی که کاربر بی‌اطلاع است، صورت می‌گیرد Coinhive.نرم‌افزاری برای کریپتوجکینگ است. ارزهای دیجیتالی که بیشتر استخراج می‌شوند، معمولاً کوین‌های حریم خصوصی با تاریخچه تراکنش‌های پنهان هستند. اگرچه این حمله مخرب با هدف سود انجام می‌شود، اما برخلاف سایر جرائم سایبری، کاملاً از دید کاربر پنهان می‌ماند. نرم‌افزارهای کریپتوجکینگ می‌توانند با تخلیه

1. Cryptojacking

منابع محاسباتی، دستگاه‌ها را کند کرده و از کار بیندازند. استخراج زنجیره بلوکی توسط دستگاه‌های آلوده را می‌توان با سخت‌افزارهای اختصاصی (مانندFPGAها وASIC ها) مقابله کرد. این روش ازنظر مصرف انرژی کارآمدتر است و ممکن است هزینه‌های کمتری نسبت به سرقت منابع محاسباتی داشته باشد.

- **حمله روز صفر (0-Day)**

این تهدید نرم‌افزاری شدید نیاز به تلاش‌های بیشتری از سوی فروشنده برای کاهش دارد. هکرها می‌توانند از این آسیب‌پذیری برای تأثیر منفی بر برنامه‌ها، داده‌ها، دستگاه‌های اضافی یا شبکه‌ها تا زمانی که مشکل برطرف شود، سوءاستفاده کنند. در ابتدا، اصطلاح «روز صفر» به‌روزهای پس از انتشار یک وصله نرم‌افزاری جدید برای عموم اشاره داشت؛ بنابراین، «نرم‌افزار روز صفر» به معنای نفوذ به دستگاه توسعه‌دهنده قبل از انتشار بود. در حال حاضر، این اصطلاح به آسیب‌پذیری‌هایی که امکان این هک را می‌دهند و تعداد روزهایی که فروشنده برای رفع آن‌ها داشته است، اشاره دارد. فروشندگانی که آسیب‌پذیری‌ها را درک می‌کنند، معمولاً وصله‌هایی ایجاد می‌کنند یا راه‌هایی برای کاهش آن‌ها توصیه می‌نمایند. هرچه فروشنده سریع‌تر از آسیب‌پذیری مطلع شود، نیاز به توسعه وصله تعمیر به صفر نزدیک می‌شود. هنگامی‌که یک مشکل رفع می‌شود، احتمال موفقیت سوءاستفاده کاهش می‌یابد، زیرا کاربران بیشتری وصله را اعمال می‌کنند. مگر اینکه یک آسیب‌پذیری به‌طور تصادفی برطرف شود، مانند یک به‌روزرسانی نامرتبط که ضعف را رفع می‌کند، احتمال اینکه کاربر یک وصله ارائه شده توسط فروشنده داشته باشد که مشکل را برطرف کند، به صفر نزدیک می‌شود، بنابراین سوءاستفاده همچنان امکان‌پذیر است.

- **حمله بروت فورث[1]**

این حمله شامل هک از طریق آزمون‌وخطا برای جمع‌آوری اعتبارنامه‌های ورود، رمزهای عبور و کلیدهای رمزنگاری است. BFA با استفاده از یک تاکتیک ساده اما قابل‌اعتماد، به دسترسی غیرمجاز به حساب‌های خصوصی و ساختارها و شبکه‌های سازمان‌ها دست می‌یابد.

1. Brute Force

- **نرم‌افزار تبلیغاتی مزاحم (Adware)**

تبلیغات پاپ‌آپ بی‌شمار روی رایانه یا دستگاه تلفن همراه می‌توانند مخرب شوند و با ربودن مرورگر فرد، باعث حجیم شدن/کند شدن آن و واردکردن ویروس‌ها یا جاسوس‌افزارها شوند.

- **جعل سرور نام دامنه** (DNS)

این حمله همچنین به‌عنوان مسمومیت حافظه پنهان سرور نام دامنه شناخته می‌شود. به داده‌های سرور نام دامنه در حافظه پنهان آن آسیب می‌زند و باعث می‌شود سرور نام یک رکورد نادرست (مانند یک آدرس IP) را بازگرداند و ترافیک را به هر رایانه‌ای که هکر انتخاب کرده است، هدایت کند؛ به‌عبارت‌دیگر، این نوع جعل نام‌های درون سرور نام‌گذاری شبکه را جهت اهداف خاص دست‌کاری کرده و هویت خود را با هویت‌های دیگر جایگزین می‌کند.

- **هکر امنیت سایبری**

یک حمله سایبری هرگونه قصد برای سرقت، افشا، تغییر، غیرفعال کردن یا تخریب داده‌ها، برنامه‌ها یا سایر دارایی‌ها با استفاده از دسترسی غیرمجاز به یک شبکه، سامانه رایانه‌ای یا دستگاه دیگر است. مهاجمان حملات سایبری را با انگیزه‌های مختلفی راه‌اندازی می‌کنند. احراز هویت دومرحله‌ای اغلب مانع از دسترسی هکرها به اطلاعات شخصی می‌شود. بااین‌حال، اطلاعات تماس واقعی برای هکرهایی که ترجیح می‌دهند از تلفن‌های زنگ‌دار، ایمیل‌های جعلی متعدد و سرویس‌های پیام‌رسانی رمزگذاری‌شده به‌درستی برای حفظ حریم خصوصی استفاده کنند، بسیار خطرناک است.

- **روتکیت**[1]

نرم‌افزار مخربی که دسترسی سطح روت (ریشه و یا به عبارتی دسترسی سطح مدیریتی) ممتاز را به دستگاه ارائه می‌دهد و درعین‌حال حضور خود را در دستگاه پنهان می‌کند، به‌عنوان روتکیت شناخته می‌شود. این نرم‌افزار مخرب می‌تواند تأثیر شدیدی بر عملکرد دستگاه بگذارد و داده‌های شخصی را در معرض خطر قرار دهد. روتکیت‌ها می‌توانند زمانی وارد رایانه‌ها شوند که کاربران ایمیل‌های اسپم را باز می‌کنند و ناخواسته نرم‌افزارهای

1. Rootkit

مخرب مانند کیلاگرها را دانلود می‌کنند که می‌توانند اطلاعات ورود کاربر را نیز ضبط کنند.

- **سرقت هویت**

سرقت هویت خطر جدی امنیت سایبری است که زمانی رخ می‌دهد که فردی اطلاعات فرد دیگری را برای سود شخصی، به‌ویژه بدون رضایت آن فرد، سرقت می‌کند. سرقت هویت جرمی است که در آن، یک مجرم از تقلب یا فریب برای به‌دست‌آوردن اطلاعات حساس از یک هدف استفاده می‌کند و از آن سوءاستفاده می‌کند تا خود را به‌جای قربانی جا بزند. معمولاً مجرمان به دنبال سود مالی هستند. چهار نوع سرقت هویت شامل سوابق پزشکی، جنایی، مالی و کودک/نوجوان می‌شود.

- **تهدیدات پایدار پیشرفته**

بهترین تعریف برای حملات APT را می‌توان از روی عنوان گذاشته‌شده بر روی این مدل حملات به‌دست‌آوردن آورد:

(A) :(Advanced) بدین معنی که مهاجمان در این مدل حملات به‌خوبی آموزش‌دیده‌اند، سازمان‌یافته‌اند، منابع مالی آن‌ها تأمین شده است و از طیف گسترده‌ای از فنّاوری‌های نفوذ به شبکه و ابزارهای دسترسی به داده‌ها و دست‌کاری داده‌ها استفاده می‌کنند.

(P):(Persistent) اشاره به پایداری حمله در طی مدت‌زمان طولانی می‌کند. مهاجمان به‌جای آنکه به دنبال دستیابی به اهداف فوری و موقت باشند به دنبال یک هدف خاص با اولویت بالا و همچنین به دنبال حفظ حضور خود به مدت طولانی در شبکه قربانی هستند (آهسته و پیوسته و هدفمند عمل‌کردن).

(T):(Threat) قصد این مهاجمان در این حملات آسیب رساندن، ایجاد اختلال در داده یا خدمات و سرقت اطلاعات خاص است. حمالت APT تحت عنوان حملات آهسته و پیوسته طبقه‌بندی‌شده‌اند. پیوسته از این نظر که ردپای بسیار کمی را از خود بر روی شبکه قربانی برجای می‌گذارند و آهسته از این نظر که مدت‌زمان اجرای آن‌ها به نسبت سایر حملات طولانی‌تر است (خسروی, ۱۳۹۹, ص.۱۷).

۵. هوش تهدیدات سایبری (CTI)

هوش تهدیدات سایبری به دانش، مهارت‌ها و آشنایی تجربی درباره حوادث و ارزیابی‌های تهدیدات سایبری و تخریب داده‌ها اشاره دارد که به کاهش حملات سایبری بالقوه و رویدادهای مضر فضای سایبری کمک می‌کند (Yaacoub et al., 2020b). هوش تهدید سایبری رویکرد جدید مبتنی بر فنّاوری‌های هوش مصنوعی است و هدف آن جمع‌آوری، تجزیه‌وتحلیل حملات فعلی و بالقوه‌ای است که امنیت یک سازمان یا دارایی‌های آن را تهدید می‌کند (پاشایی, ۱۴۰۳, ص.۳۵).

منابع این هوش شامل هوش منبع باز، رسانه‌های اجتماعی هوشمند، شناخت انسانی، استعداد فنی، آرشیوهای ثبت سخت‌افزار، شواهد یا مدارک جمع‌آوری‌شده از ترافیک اینترنت و اطلاعات وب عمیق/تاریک است. در سال‌های اخیر، این هوش به یک استراتژی امنیت سایبری حیاتی برای شرکت‌ها و سازمان‌ها تبدیل شده است، زیرا در فرایند پیشگیری از حملات بهتر عمل می‌کند و تعیین می‌کند که کدام خطرات بیشترین ریسک تجاری را دارند؛ بنابراین، شرکت‌ها و سازمان‌هایی که در خط مقدم قرار دارند، فعالانه سعی می‌کنند نقاط ضعف خود را کشف کنند و از حملات سایبری قبل از وقوع جلوگیری کنند. به دلیل اینکه رایج‌ترین روش هک از طریق بهره‌برداری از تهدیدات است، این روش بسیار پرکاربرد شده است. به همین علت، نیاز است هوش تهدیدات سایبری موردبررسی قرار گیرد. در ادامه به چرخه هوش تهدیدات سایبری که به‌عنوان معماری آن نیز شناخته می‌شود آورده شده است. فرآیند پنج مرحله‌ای توسعه یا چرخه هوش تهدیدات سایبری که به‌صورت دایره‌ای و پیوسته است (در شکل ۲ نمایش داده شده است)، به شرح زیر است (Davidson, 2020, p. 3):

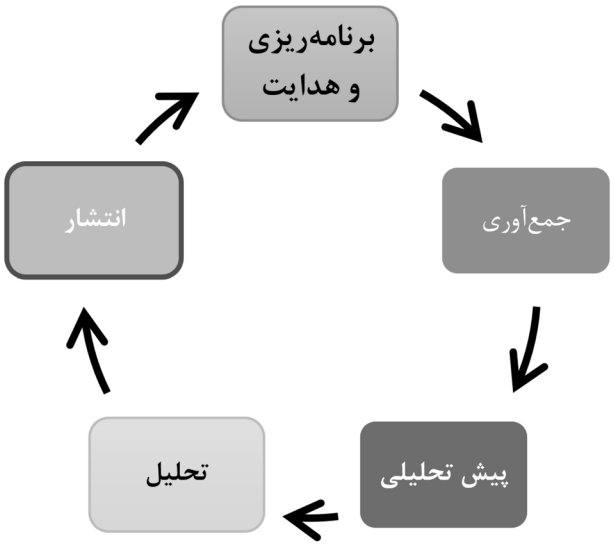
۱) **برنامه‌ریزی و هدایت** به این معنی است که مصرف‌کننده محصول هوشمند باید یک موضوع یا هدف خاص را بداند، برای آن هدف، تهدیدات را استخراج نماید و برای هر تهدید برنامه‌ریزی نماید و هدایت جلوگیری از آن را انجام دهد.

۲) **جمع‌آوری** با دسترسی به اطلاعات خام حیاتی برای ایجاد محصول هوشمند نهایی آغاز می‌شود؛ به‌عبارت‌دیگر، برای رسیدن به هدفی که در بند ۱ بیان‌شده است نیاز است داده‌ها و اطلاعاتی جمع‌آوری شود.

۳) **مرحله پردازش (یا پیش‌تحلیلی)** داده‌های خام را از طریق روش‌هایی مانند رمزگشایی، ترجمه، کاهش ابعاد و غیره فیلتر و آماده تحلیل می‌کند. ازآنجاکه داده‌ها هوشمند نیستند، تبدیل‌ها، پردازش و تحلیل موردنیاز است.

۴) **مرحله تحلیل** داده‌های آماده‌شده را به اطلاعات و دانش تبدیل می‌کند.

۵) **مرحله انتشار** نتایج هوش تهدید یافت شده را به کاربران مختلف ارسال می‌کند.



شکل ۲. چرخه هوش تهدیدات سایبری (Davidson, 2020, p. 3)

در این چرخه موردی که باید در هرکدام از مرحله باید مدنظر قرارداد، ارزیابی آن مرحله است. به‌طورکلی سه سطح اساسی در هوش تهدیدات سایبری برای ارزیابی تهدیدات به شرح بیان‌شده است (Veith et al., 2019, p. 4):

۱) تاکتیکی

به شناسایی بازیگران تهدیدات سایبری با استفاده از شاخص‌های سازش (مانند دامنه‌های اینترنتی، آدرس‌های IP یا هش‌ها) کمک می‌کند، اگرچه تحلیل «تاکتیک‌ها، تکنیک‌ها و روش‌ها» مورداستفاده توسط مجرمان سایبری در مراحل اولیه است.

بینش‌های ایجادشده در این سطح می‌تواند به گروه‌های امنیتی کمک کند تا به‌طور فوری حملات سایبری آینده را پیش‌بینی و شناسایی کنند.

۲) عملیاتی

این سطح از ارزیابی فنی‌ترین سطح است که جزئیات پیچیده و خاص حملات، منطق، مهارت‌های بازیگران تهدیدات سایبری و کمپین‌های فردی را به اشتراک می‌گذارد. تخصص در این سطح شامل ماهیت، قصد و زمان‌بندی تهدیدات سایبری نوظهور است که چالش‌برانگیزتر است و اغلب از انجمن‌های وب عمیق، مبهم و غیرقابل‌دسترس برای گروه‌های داخلی به‌دست‌آوردن می‌آید. متخصصان امنیت در پاسخ به حملات از این هوش عملیاتی استفاده می‌کنند.

۳) راهبردی

هدف این است که ریسک‌های تجاری فعلی و پیش‌بینی‌شده و پیامدهای تهدیدات سایبری بالقوه را بررسی کند تا به رهبران و مخاطبان غیرفنی کمک کند پاسخ‌های خود را اولویت‌بندی کنند.

استفاده از این هوش به سازمان‌ها، مؤسسات یا سایر افراد اجازه می‌دهد تا وضعیت‌های امنیت سایبری پیشگیرانه و قوی‌ای ایجاد کنند تا کل سیاست‌های مدیریت ریسک و امنیت سایبری را تقویت کنند و به‌سمت امنیت سایبری پیش‌بینانه و پیشگیرانه به‌جای صرفاً واکنش به یک حمله سایبری حرکت می‌کند؛ به‌عبارت‌دیگر سازمان را از حالت منفعلانه به حالت پیش‌دستانه در برابر حملات سایبری قرار می‌دهد و اطلاعات و بینش‌های زمینه‌ای درباره حملات سایبری فعال و تهدیدات سایبری بالقوه را برای کمک به تصمیم‌گیری ارائه می‌دهد. مزایای هوش تهدیدات سایبری به‌صورت زیر خلاصه نمود (Hussaini et al., 2022, p. 9):

- از نقض داده‌ها با آزادکردن اطلاعات حساس جلوگیری می‌کند، بنابراین ازدست‌دادن داده‌ها جلوگیری می‌نماید.
- هزینه‌ها را کاهش می‌دهد، زیرا نقض داده‌ها هزینه دارد و کاهش خطر آن‌ها به صرفه‌جویی در هزینه کمک می‌کند.

- به مؤسسات کمک و راهنمایی می‌کند تا اقدامات امنیت سایبری را برای محافظت در برابر حملات سایبری آینده اجرا کنند.
- به جامعه امنیت سایبری اجازه می‌دهد تا دانش، مهارت‌ها و تجربه را به اشتراک بگذارند.
- به شناسایی سریع‌تر و بهتر تهدیدات سایبری، سازکارهای تحویل، شاخص‌های سازش در سراسر زیرساخت و بازیگران و محرک‌های خاص بالقوه کمک می‌کند.
- در تشخیص حملات سایبری در طول و قبل از این مراحل کمک می‌کند.
- شاخص‌هایی از اقدامات انجام شده در هر مرحله از حمله را ارائه می‌دهد.
- سطوح تهدید، بردارهای حمله و فعالیت‌های مخرب را به پلتفرم‌های فنّاوری اطلاعات و عملیاتی ارتباط می‌دهد.
- به‌عنوان یک مخزن مبتنی بر واقعیت برای شواهد حملات سایبری موفق و ناموفق عمل می‌کند.
- شاخص‌هایی را برای گروه‌های پاسخ اضطراری و آلودگی ارائه می‌دهد.

سه عنصر کلیدی باید در هوش تهدیدات سایبری وجود داشته باشد (Gurjanov et al., 2022, p. 11):

- **مبتنی بر شواهد:** هر اعتبارسنجی هوشمند باید ابتدا از روش‌های مناسب جمع‌آوری شواهد ناشی شود. سایر فرآیندها، مانند تحلیل بدافزار، می‌توانند هوش تهدیدات سایبری را افزایش دهند.
- **کارایی:** برای اینکه هوش تهدیدات سایبری بتواند به‌طور مثبت پیامدهای رویداد امنیت سایبری را اصلاح کند، هوش باید رفتارها و روش‌های خاص را در مورد زمینه و داده‌ها روشن کند.
- **قابل اقدام:** اقدام از اطلاعات هوش تهدیدات سایبری ناشی می‌شود تا به مقابله و حذف حملات سایبری منجر شود.

با توجه به موارد بیان‌شده هوش تهدیدات سایبری را می‌توان در سه حوزه تقسیم‌بندی نمود: مبتنی بر امضا، مبتنی بر رفتار و مبتنی بر یادگیری ماشین. نکته حائز اهمیت این است

که نمی‌توان همه موارد را در مبتنی بر یادگیری ماشین خلاصه نمود و لذا این دسته‌بندی صورت‌گرفته است که در ادامه هرکدام از این دسته‌ها شرح داده می‌شود.

هوش تهدیدات سایبری سنتی که مبتنی بر امضا معرفی شده است، عمدتاً بر ردیابی شاخص‌های تهدید شناخته‌شده مانند آدرس‌های IP و نام‌های دامنه تمرکز کرده است، ممکن است ارزش بلندمدتی برای دفاع در برابر این نوع تهدیدات و حملات در حال تکامل ایجاد نکند. چارچوب نرده‌ای[1] به‌عنوان یکی از رویکردهای نوین در بهبود امنیت سایبری و ارزیابی عملکرد سامانه‌ها در برابر این نوع تهدیدات مطرح است. این چارچوب یک چارچوب استخراج دانش است که می‌تواند الگوهای حمله مبتنی بر متن را از گزارش‌های هوش تهدیدات سایبری استخراج کند و با به تصویر کشیدن مراحل حمله در شبکه‌های اندروید و سازمانی، الگوهای حمله را مشخص کرده و آن‌ها را به‌طور سامانمند به چارچوب الگوهای حمله میتره[2] نقشه‌برداری می‌کند. این روش به روش‌های مبتنی بر رفتار (الگو) شناخته می‌شود. با وجود مزایای چارچوب نرده‌ای در بهبود امنیت سایبری و شناسایی الگوهای حملات پیچیده، این چارچوب با برخی محدودیت‌ها و چالش‌ها مواجه است که می‌تواند بر عملکرد و دقت آن تأثیر منفی بگذارد. لذا با توجه به پیچیدگی حملات سایبری پیشرفته، بهبودهای بیشتری مانند ادغام لاگ‌های سامانه، ارزیابی عملکرد در مجموعه داده‌های بزرگ و افزودن تحلیل‌های زمانی به چارچوب نرده‌ای، برای افزایش کارآمدی این چارچوب پیشنهاد می‌شود. این بهبودها می‌توانند به افزایش دقت، کارایی و انعطاف‌پذیری این چارچوب در مقابله با تهدیدات سایبری پیشرفته منجر شوند (پاشایی, ۱۴۰۳, ص.۴۷).

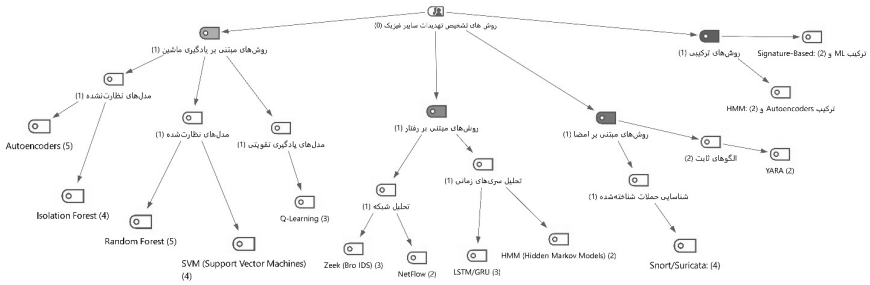
استفاده از یادگیری ماشین به‌عنوان یکی از اجزای مهم دایره هوش مصنوعی است. به‌طوری‌که در استخراج داده و تحلیل لاگ‌های امنیتی از سامانه‌های فنّاوری اطلاعات، سازمان‌ها به دنبال راه‌حل‌های خودکار برای تشخیص تهدیدات سایبری می‌گردند. یادگیری ماشین به‌عنوان یکی از رویکردهای اساسی جهت کاهش هزینه‌ها در تجزیه‌وتحلیل امنیتی به‌شمار می‌رود. چالش اصلی این حوزه، انتخاب الگوریتم مناسب یادگیری ماشین برای تجزیه لاگ‌های امنیتی، به‌ویژه در محیط‌های بزرگ SOC است. یادگیری ماشین در پیش‌بینی حملات سایبری و همچنین تأمین امنیت بسیار کارا

1. LADDER
2. MITRE ATTACK

به‌شمار می‌آید. اثربخشی یادگیری ماشین از طریق تحقیقات و داده‌های جمع‌آوری‌شده از مجموعه مایکروسافت تأیید شده است. به‌طور هم‌زمان، پیاده‌سازی سامانه‌های هوش مصنوعی به‌منظور شناسایی و پیشگیری از تهدیدات، با بهره‌گیری از شبکه‌های عصبی و مدل‌های هوش مصنوعی، برای بهبود امنیت سایبری و افزایش قابلیت اطمینان سامانه اقدامی حیاتی به‌شمار می‌آید. همچنین، روش‌های پیش‌بینی با استفاده از الگوریتم «سری‌های زمانی» و مدل "SARIMA" به‌دقت و کارایی مناسبی منجر می‌شوند. این ترکیب از یادگیری ماشین در زمینه امنیت سایبری، امکان شناسایی و پیشگیری از تهدیدات پیچیده و چالش‌برانگیز را فراهم می‌کند و از اهمیت چشمگیری برخوردار است (نریمانی و همکاران۱۴۰۲, . ص.۱).

۶. روش‌های تشخیص مبتنی بر مصاحبه

علیرغم اینکه در سال‌های اخیر سامانه‌های سایبرفیزیک بسیار پرکاربرد شده‌اند و در اکثر سازمان‌ها و شرکت‌ها از این سامانه‌ها استفاده می‌نمایند ولی متأسفانه در جامعه علمی کشور هنوز مدنظر قرار نگرفته است و همان‌طور که در بخش قبل بیان شد از ۶ نفر متخصص در این حوزه سؤالات مصاحبه پرسیده شده است. سؤالات به‌صورت نیمه‌ساختاریافته تهیه‌شده و به‌صورت تایپ‌شده در اختیار مصاحبه‌شوندگان قرارگرفته و سپس جمع‌آوری‌شده است و در نرم‌افزار MaxQDA کدگذاری شده است. به دلیل اینکه در این تحقیق اهداف فرعی تقسیم‌بندی شده است فرایند کدگذاری در این نرم‌افزار به‌صورت محوری انجام شده است. فرایند اعتبارسنجی و پایایی نیز با استفاده از بازبینی همکار مورد ارزیابی قرارگرفته شده است و به همین علت دسته‌بندی اصلی به همراه روابط بین آن‌ها استخراج می‌شود که نتایج آن به شرح شکل ۳ آورده شده است.



شکل ۳. روش‌های تشخیص تهدیدات به سامانه‌های سایبرفیزیک با استفاده از هوش مصنوعی

سامانه‌های سایبر-فیزیکی به دلیل پیوند عمیق بین اجزای فیزیکی و سایبری، در معرض تهدیدات پیچیده‌ای قرار دارند که می‌توانند عواقب فیزیکی به دنبال داشته باشند (مانند تخریب تجهیزات صنعتی یا اختلال در شبکه‌های حیاتی). برای مقابله با این چالش‌ها، همان‌گونه که در شکل ۳ نمایش داده شده است ترکیبی از روش‌های تشخیص مبتنی بر یادگیری ماشین، تحلیل رفتاری و امضاهای امنیتی ضروری است. در جدول ۲، نتایج به‌دست‌آمده را با جزئیات کامل‌تر آورده شده و برای هرکدام مثال کاربردی نیز بیان‌شده است.

جدول ۲. روش‌ها، مزایا و معایب تشخیص تهدیدات به سامانه‌های سایبرفیزیک توسط هوش مصنوعی

روش	مزایا	معایب	کاربردهای کلیدی
یادگیری نظارت‌شده	دقت بالا در حملات شناخته‌شده (۹۵٪+ در داده‌های متعادل)	نیاز به داده‌های برچسب‌دار و به‌روز	تشخیص حملات False Data Injection در حسگرها صنعتی
یادگیری نظارت‌نشده	شناسایی حملات ناشناخته (Zero-Day)	نرخ بالای False Positive در داده‌های پرنویز	کشف ناهنجاری در داده‌های توربین‌های بادی با Autoencoders
مبتنی بر تحلیل امضا	سرعت بالا و مصرف منابع کم	عدم شناسایی حملات جدید	تشخیص Malware های صنعتی مانند Havex در پروتکل‌های OPC UA
مبتنی بر تحلیل رفتار	انعطاف‌پذیری در مواجهه با حملات پیچیده	نیاز به مدل‌سازی دقیق رفتار عادی سامانه	شناسایی حملات Replay در سامانه‌های کنترل ترافیک هوایی با LSTM

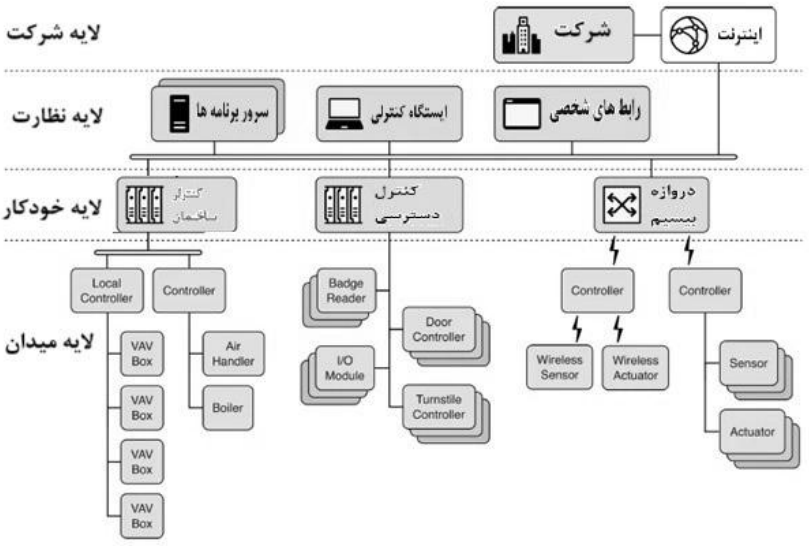
یافته‌های کلیدی از پژوهش‌های اخیر و مصاحبه‌های انجام شده نشان می‌دهد که برای اثربخشی یادگیری عمیق در سامانه‌های سایبرفیزیک، در برابر حملات از پیش

شناخته‌شده مانند حمله DDos استفاده از مدل‌ها و الگوریتم‌های با نظارت مانند الگوریتم جنگل تصادفی بیشترین (و درخت تصمیم) کاربرد را دارد و در تشخیص حملات مشخص بسیار خوب عمل می‌کنند (خرم و رحمانی منش, ۱۴۰۲, ص.۶).

در کشف حمله روز صفر استفاده از یادگیری بدون نظارت کارایی بیشتری نسبت به یادگیری با ناظر دارد. به‌طورکلی برای شناسایی حملات جدید استفاده از روش‌های یادگیری ماشین بدون ناظر مدنظر است. در سامانه‌های بلادرنگ و زمان واقعی که تأخیر عامل بسیار حیاتی است روش‌های تحلیل امضا کاربرد دارد و بااینکه دقت شناسایی حملات جدید را ندارد ولیکن زمان پاسخ‌دهی این روش در سامانه‌های سایبرفیزیک تأخیر ایجاد نمی‌کند. برای اینکه بتوان دقت و کیفیت تشخیص در هرکدام از تهدیدات را بالاتر برد (البته با صرف هزینه بیشتر) استفاده از روش‌های ترکیبی پیشنهاد می‌شود.

پیاده‌سازی سامانه تشخیص تهدیدات سایبری بر سامانه‌های سایبرفیزیک با استفاده از هوش مصنوعی

برای استقرار یک سامانه تشخیص تهدیدات مؤثر در سامانه‌های سایبر-فیزیکی، باید به ملاحظات فنی، محدودیت‌های منابع و الزامات بلادرنگ توجه کرد. در این بخش، راه‌کارهای عملی را به‌صورت گام‌به‌گام و با ذکر ابزارها و تکنیک‌های قابل‌اجرا ارائه می‌کنیم. همان‌گونه که در بخش ۴ این مقاله عنوان‌شده در ابتدای پیاده‌سازی نیازمند برنامه‌ریزی است که به‌عنوان طرح‌ریزی معماری سامانه تشخیص تهدیدات معرفی می‌شود. این معماری بر اساس پیشنهاد مرکز NIST در شکل ۴ نمایش داده شده است. این سند با نام سند NIST SP 800-82 معرفی شده است (Jillepalli et al., 2017, pp. 1-4).



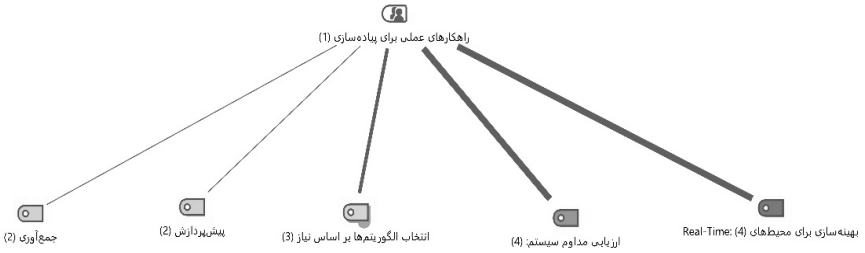
شکل ۴. معماری پیاده‌سازی سامانه تشخیص تهدیدات سایبری

با توجه به چرخه بیان‌شده در شکل ۲ و روش‌های تشخیص بیان‌شده در شکل ۳ و معماری بیان‌شده در بالا نیاز است در حین اجرای فرایند تشخیص برخی از مسائل را مدنظر قرارداد که عبارتند از:

- اطلاعات حساس نیاز به محافظت دارند تا ازدست‌دادن داده‌ها جلوگیری شود.
- ازآنجاکه نقض داده‌ها به معنای هزینه است، کاهش خطر نقض داده‌ها باعث صرفه‌جویی در هزینه می‌شود.
- سازمان‌ها برای اجرای اقدامات امنیت سایبری برای جلوگیری از حملات سایبری آینده به کمک نیاز دارند.
- جامعه امنیت سایبری باید دانش، مهارت‌ها و تجربیات را به اشتراک بگذارد.
- شناسایی تهدیدات سایبری به بهبود ابزارهای تحویل، شاخص‌ها، بازیگران و محرک‌های خاص آینده کمک می‌کند.
- تشخیص حملات سایبری در طول و قبل از مراحل سامانه سایبرفیزیک.
- ارائه شاخص‌هایی از اقدامات انجام شده در هر مرحله از حمله.

- ارسال اطلاعات درباره سطوح تهدید، بردارهای حمله و فعالیت‌های مخرب به پلتفرم‌های فنّاوری اطلاعات و ارتباطات.
- به‌عنوان یک مخزن شواهد برای حملات سایبری موفق و ناموفق عمل می‌کند.
- شاخص‌هایی را برای گروه‌های پاسخ اضطراری سخت‌افزاری و گروه‌های پاسخ به حوادث ترتیب می‌دهد.

راه‌کار عملی پیاده‌سازی یکی دیگر از پرسش‌های مصاحبه است که متخصصین برای پیاده‌سازی سامانه تشخیص پرسیده شده است همان‌گونه که در شکل ۵ نشان‌داده شده است، پس از کدگذاری، مشخص گردید که اکثر مصاحبه‌شوندگان (۴ نفر) بهینه‌سازی و ارزیابی مداوم را بیشترین اثر در پیاده‌سازی سامانه تشخیص تهدیدات سایبری بر سامانه‌های سایبرفیزیک بر اساس هوش مصنوعی می‌دانند.



شکل ۵. راه‌کارهای عملی برای پیاده‌سازی سامانه تشخیص تهدیدات سایبری

۹. نتیجه‌گیری و پیشنهادها

این مقاله به بررسی لایه‌های مختلف «سامانه‌های سایبرفیزیکی» می‌پردازد و به‌طور خلاصه به بررسی تهدیدات سایبری متصور به سامانه‌های سایبرفیزیک پرداخته و روش‌های تشخیص این تهدیدات را با استفاده از هوش مصنوعی بیان کرده است. روش‌های بررسی‌شده در اینجا برای غلبه بر محدودیت‌های فعلی با استفاده از پیشرفته‌ترین فنون تشخیص و محافظت پویا و انطباقی با نگاه بر توسعه فنّاوری‌ها هستند. چندین تهدید رایج لایه سامانه سایبرفیزیک و مسائل تحقیقاتی حل‌نشده در توسعه اقدامات امنیتی هوشمند این سامانه‌ها توسط روش‌های امنیتی مبتنی بر هوش مصنوعی معرفی‌شده‌اند (Mahmoud et al., 2019, pp. 5-6)، درنهایت نشان‌داده شده است که تهدیدات به

سامانه‌های سایبرفیزیکی بسیار پیچیده هستند زیرا تمام فنّاوری‌های لازم از قبل در جای خود قرار دارند. یکی از مهم‌ترین چالش، انقلاب فنّاوری جدید شامل اتصال چندین سامانه سایبرفیزیکی برای انجام وظایف مستقل در یک محیط فشرده است و لذا هوش مصنوعی به‌عنوان ابزار کلیدی برای افزایش ادغام سامانه‌های سایبرفیزیکی در سامانه هوشمند که نیاز به تلاش دستی کمی دارد، برجسته می‌شود. با توجه به بررسی به‌عمل‌آمده بسته به نوع تهدید نوع استفاده از هوش برای تشخیص متفاوت است ولی می‌توان در سه دسته کلی و یک دسته ترکیبی تقسیم‌بندی نمود.

نکته مورد اهمیت این است که جمع‌آوری و پیش‌پردازش داده‌ها در عمل باید منجر به استفاده از دیتاست‌های استاندارد شود. به‌طور مثال اکثر تحقیقات اولیه برای داده‌های مرتبط با حملات به شبکه از دیتاست CICIDS2017 [۱] و یا برای داده‌های صنعتی از دیتاست SWaT [۲] استفاده می‌کنند. به دلیل کامل بودن این دیتاست‌ها قابلیت استفاده در راستای تشخیص تهدیدات سایبری بر سایبرفیزیک را دارند.

انتخاب الگوریتم به‌عنوان یکی از الزامات اولیه انتخاب نوع هوش مصنوعی مورداستفاده در فرایند تشخیص تهدید است و همان‌طور که در جدول ۲ نشان‌داده شده است تقریباً برای هر نوع حمله‌ای الگوریتمی خاص بهره بیشتری دارد و به‌طور مثال برای حملات شناخته‌شده SVM + Signature-Based و حملات ناشناخته+ Isolation Forest Autoencoders پیشنهاد می‌شود. برای بهینه‌سازی محیط‌های زمان واقعی با استفاده از کاهش ابعاد داده از PCA برای افزایش سرعت پردازش و از سخت‌افزارهای ویژه مانند FPGA در پیاده‌سازی مدل‌های LSTM استفاده شود. درنهایت سامانه‌ها بایستی به‌صورت مداوم مورد ارزیابی قرار گیرد به‌طوری‌که مقدار نرخ تشخیص [۳] بالای ۹۵٪ و مقدار نرخ شناسایی خطا [۴] کمتر از ۵٪ باشد؛ به‌عبارت‌دیگر بایستی بالای ۹۵ درصد حملات

---

۱. یکی از معروف‌ترین و پراستفاده‌ترین دیتاست‌های عمومی برای تحقیق در زمینه تشخیص نفوذ و امنیت شبکه است. این دیتاست توسط موسسه سایبرسیکوریتی کانادا (CIC) توسعه داده شده و شامل ترافیک شبکه واقعی و حملات متداول است.

۲. یکی از دیتاست‌های معروف در حوزه امنیت سایبری سامانه‌های صنعتی است که برای تحقیق در مورد تشخیص نفوذ در محیط‌های عملیاتی صنعتی طراحی شده. این دیتاست توسط مرکز تحقیقات سایبری iTrust در دانشگاه سنگاپور (SUTD) توسعه و بر پایهٔ یک سیستم واقعی تصفیه آب شبیه‌سازی شده است.

3. Detection Rate (DR)

4. False Positive Rate (FPR)

شناسایی شود و مقدار خطای سامانه نیز کمتر از ۵ درصد باشد. به‌طورکلی نتیجه می‌شود که تجهیزات موجود در صورت بهینه‌سازی و ارزیابی مداوم امکان تشخیص عملی تهدیدات سایبری بر سامانه‌های سایبرفیزیک را دارند.

منابع

- Alowaidi, M., Sharma, S. K., AlEnizi, A., & Bhardwaj, S. (2023). Integrating artificial intelligence in cyber security for cyber-physical systems. **Electronic Research Archive**, **31**(4).
- Baheti, R., & Gill, H. (2011). Cyber-physical systems. **The Impact of Control Technology**, **12**(1), 161-166.
- Carreras Guzman, N. H., Wied, M., Kozine, I., & Lundteigen, M. A. (2020). Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. **Systems Engineering**, **23**(2), 189-210.
- Davidson, R. (2020). Cyber-physical production networks, artificial intelligence-based decision-making algorithms, and big data-driven innovation in Industry 4.0-based manufacturing systems. **Economics, Management, and Financial Markets**, **15**(3), 16-22.
- Erbschloe, M. (2004). **Trojans, worms, and spyware: A computer security professional's guide to malicious code**. Elsevier.
- Fitzgerald, J., Larsen, P. G., & Pierce, K. (2019). Multi-modelling and co-simulation in the engineering of cyber-physical systems: Towards the digital twin. In **From Software Engineering to Formal Methods and Tools, and Back: Essays Dedicated to Stefania Gnesi on the Occasion of Her 65th Birthday** (pp. 40-55). Springer.
- Gurjanov, A. V., Babenkov, V. I., Zharinov, I. O., & Zharinov, O. O. (2022). **Cyber-physical systems control principles and congregation of resources for a centralized and decentralized artificial intelligence**. **2373**(6), 062017.
- Hussaini, A., Qian, C., Liao, W., & Yu, W. (2022). **A taxonomy of security and defense mechanisms in digital twins-based cyber-physical systems**. 597-604.
- Jillepalli, A. A., Sheldon, F. T., de Leon, D. C., Haney, M., & Abercrombie, R. K. (2017). **Security management of cyber physical control systems using NIST SP 800-82r2**. 1864-1870.
- Mahmoud, M. S., Hamdan, M. M., & Baroudi, U. A. (2019). Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges. **Neurocomputing**, **338**, 101-115.
- Szor, P. (2005). **The art of computer virus research and defense**. Pearson Education.

- Veith, E. M., Fischer, L., Tröschel, M., & Nieße, A. (2019). **Analyzing cyber-physical systems from the perspective of artificial intelligence**. 85-95.
- W. Duo, M. Zhou, & A. Abusorrah. (2022). A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. **IEEE/CAA Journal of Automatica Sinica**, **9**(5), 784-800. https://doi.org/10.1109/JAS.2022.105548
- Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020a). Cyber-physical systems security: Limitations, issues and future trends. **Microprocessors and Microsystems**, **77**, 103201.
- Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020b). Cyber-physical systems security: Limitations, issues and future trends. **Microprocessors and Microsystems**, 77, 103201.
- Zang, T., Tong, X., Li, C., Gong, Y., Su, R., & Zhou, B. (2025). Research and Prospect of Defense for Integrated Energy Cyber-Physical Systems Against Deliberate Attacks. **Energies**, **18**(6). https://doi.org/10.3390/en18061479
- پاشایی، ا. (۱۴۰۳). **استخراج TTP های حملات با کمک یادگیری ماشین**. دانشگاه صنعتی شاهرود.
- خرم، م.، رحمانی منش، م. (۱۴۰۲). **سامانه تشخیص حملات DDOS با استفاده از روش دسته‌بندی گروهی و رویکرد یادگیری فعال**.
- خسروی، م. (۱۳۹۹). **مدل‌سازی و تشخیص حملات سایبری مبتنی بر تهدیدات پایدار پیشرفته (APT)**. دانشگاه اصفهان.
- لک، م. (۱۴۰۰). **تحلیل تأثیر تهدیدات سایبری بر امنیت ملی جمهوری اسلامی ایران**. دانشگاه اصفهان.
- نریمانی، احسان، لطفی، فریده و هدایتی، سبحان. (۱۴۰۲). مروری بر کاربردهای یادگیری ماشین در مرکز عملیات امنیت و تشخیص حملات. **پژوهش‌های کاربردی در فنی و مهندسی**، **۳۲**(۴)، ۲۲۵-۲۱۱.