طبقه‌بندی جامع حوادث امنیت سایبری در سیستم‌های کنترل صنعتی

اردلان الیاسی

شرکت برق منطقه‌ای مازندران و گلستان ، ساری ، ایران

a.elyasi@mail.ir

عارفه ابراهیمی قادیکلایی

اداره آموزش و پرورش مازندران ، ساری، مازندران، ایران
arefehebrahimi@gmail.com

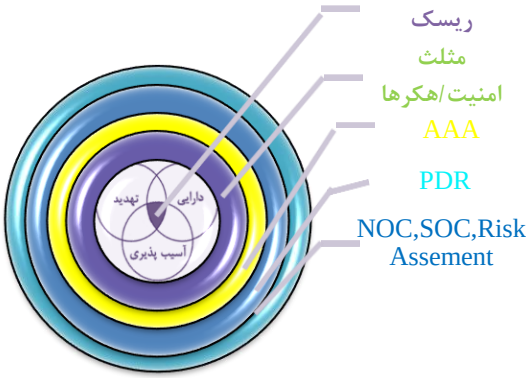
چکیده

همگرایی سیستم‌های کنترل صنعتی (ICS) با فناوری‌های اطلاعاتی، میزان در معرض‌بودن زیرساخت‌های حیاتی را در برابر تهدیدات پیشرفته‌ی سایبری–فیزیکی افزایش داده است. رویکردهای موجود در طبقه‌بندی رخدادهای امنیت سایبری، غالباً قادر به پوشش ویژگی‌های عملیاتی، معماری و ایمنی‌محور خاص محیط‌های صنعتی نیستند. در این مقاله، یک چارچوب طبقه‌بندی سلسله‌مراتبی (HTF) برای تحلیل نظام‌مند حوادث امنیت سایبری در سیستم‌های کنترل صنعتی و اسکادا ارائه می‌شود. این چارچوب با تفکیک دقیق مفاهیمی نظیر تهدید، رویداد، حادثه امنیتی، حادثه غیرتهاجمی و حمله، و با بهره‌گیری از ۲۲ پارامتر تخصصی متناسب با ICS ــ شامل منبع حمله، اقدام عملیاتی، لایه کنترلی هدف، بخش صنعتی، شدت اثر، نقض اصول سه‌گانه CIA، آسیب‌پذیری‌های بهره‌برداری‌شده و تکنیک‌های مهاجم ــــ امکان تحلیلی دقیق‌تر را فراهم می‌سازد. کارایی چارچوب پیشنهادی با طبقه‌بندی ۲۶۸ حادثه امنیتی گزارش‌شده از بازه زمانی ۱۹۸۲ ارزیابی شده و نتایج نشان می‌دهد که HTF با افزایش انسجام، قابلیت توسعه و عمق تحلیلی، از تصمیم‌گیری امنیتی، ارزیابی ریسک و پاسخ به حوادث در زیرساخت‌های صنعتی ایمنی‌محور پشتیبانی می‌کند.

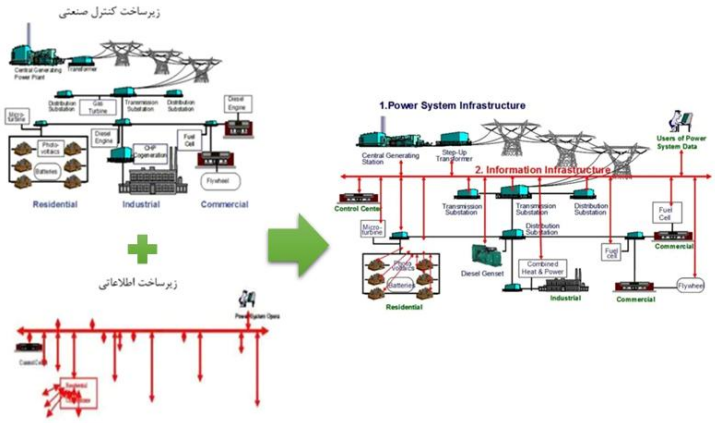
واژگان کلیدی: سیستم‌های کنترل صنعتی،اسکاد، امنیت سایبری–فیزیکی، طبقه‌بندی حوادث،رده‌بندی تهدیدات،حفاظت از زیرساخت‌های حیاتی.

۱– مقدمه

امروزه مسائل مختلفی در دنیای فیزیکی وجود دارد که توسط سیستم‌های کامپیوتری کنترل می‌شوند. این موارد مهم در کاربردهای مختلف با یکدیگر ارتباط برقرار می‌کنند که ساختار امنیت در این سیستم‌ها در شکل ۱ نشان داده شده است. سیستم‌های کنترل صنعتی یکی از مهمترین این کاربردها هستند که زیرساخت‌های حیاتی مانند نیروگاه‌ها، نفت و کارخانه‌های شیمیایی و سیستم‌های حمل و نقل را کنترل می‌کنند و سیستم‌های کنترل صنعتی ترکیبی از زیرساخت کنترل صنعتی و زیرساخت اطلاعاتی هستند(شکل ۲) و بزرگترین زیرگروه سیستم کنترل صنعتی[1]، سیستم اسکادا[2] است. اسکادا مفهوم مهمی از زیرساخت‌های حیاتی کشورها هستند و بنابراین برای امنیت ملی مهم می‌باشند. امروزه سیستم‌های کنترل صنعتی به شدت با سایرشبکه‌های سازمان و اینترنت در ارتباط هستند. آنها همچنین از فناوری‌های استاندارد مانند پروتکل ارتباطیTCP/IP استفاده می‌کنند.



شکل۱ : ساختار امنیت در سیستم‌ها



شکل ۲ : سیستم‌های صنعتی امروزی

ویژگی‌های ذکرشده دربالا، سیستم کنترل صنعتی را به یک هدف ایده‌آل برای حملات سایبری- فیزیکی تبدیل می‌کند. نقش حیاتی این سیستم‌ها منجر به اهمیت امنیت فیزیکی سایبری آنها می‌شود. به عنوان مثال،استاکس‌نت که به عنوان یک حمله هدفمند بسیار پیشرفته طراحی شده بود،آسیب‌پذیری‌های سیستم کنترل صنعتی را نشان می‌دهد که آن آسیب‌ها به عنوان شکاف‌هایی عمل کردندکه مهاجمان آن را تخریب نمودند.

---

[1]ICS
[2]SCADA(کنترل نظارتی و جمع آوری داده ها)

تلاش‌های زیادی برای دسته‌بندی حوادث امنیتی صورت گرفته است. بخش بعدی را با بررسی مختصر دسته‌بندی‌های علمی-کاربردی برجسته برای تهدیدات، حملات و حوادث امنیتی آغاز می‌کنیم. سپس تعاریفی ارائه می‌کنیم که ما در فهم دسته‌بندی کمک کند. و در نهایت، سه دسته‌بندی برجسته را مقایسه می‌کنیم.

۲- کارهای مرتبط:

در برخی منابع، مانند[۲ISA/IEC-62443](قبلاً ISA-99 یا ANSI/ISA-99)،حملات به چهار کلاس دسته‌بندی شدند: (۱) حملات فعال، (۲) حملات غیرفعال، (۳) حملات داخلی و (۴) حملات خارجی . روف و همکاران [۳] « مدل دسته‌بندی متعامد سه » را برای تهدیدات امنیتی پیشنهاد کردند که تهدیدها را به ابعادی با عنوان انگیزه، محلی‌سازی و عامل طبقه‌بندی می‌کند. ساندرو و همکاران [۱] یک مدل ترکیبی به نام « طبقه‌بندی مکعب تهدید امنیتی سیستم اطلاعاتی » یا مدل C[3] پیشنهاد کردند. ایده اصلی پشت این مدل استفاده از معیارهای دسته‌بندی ضروری و مفید است. این سه معیار اصلی عبارتند از فراوانی تهدید ، ناحیه فعالیت تهدید و منبع تهدید.

الحبیب و همکاران « هرم طبقه‌بندی تهدیدات امنیت اطلاعات » را در [۴] برای طراحی طبقه‌بندی که می‌تواند تهدیدهای عمدی را به روشی پویا طبقه‌بندی کند تا هر تهدید را در مناطق مختلف سیستم نشان دهد، پیشنهاد کرد. این مدل بر اساس سه عامل مهم ساخته شده است: دانش قبلی مهاجم (یعنی آگاهی از منشا تهدید) در مورد سیستم، حساسیت منطقه که ممکن است تحت‌تاثیر آن تهدید قرار گیرد و زیان ناشی از تهدید بر اساس اصل امنیتی[۳] CIA . شیری [۵] تهدیدها را به چهار دسته کلی تقسیم می‌کند: (۱) افشای / دسترسی غیرمجاز به اطلاعات، (۲) فریب‌کاری، یا پذیرش داده‌های نادرست، (۳) اختلال، وقفه، یا جلوگیری از عملکرد صحیح، و (۴) غصب،یا کنترل غیرمجاز بخشی از یک سیستم. بیشاپ [۶] براین باور است که این چهار طبقه، تهدیدهای رایج بسیاری را دربر می‌گیرد. بر اساس این طبقه‌بندی، بیشاپ جاسوسی، اصلاح یا تغییر، مخفی‌کاری یا جعل، انکار مبدأ، انکار دریافت، انکارخدمات (DoS)[۴] یا تاخیر را تعریف کرد.

مایکروسافت طبقه‌بندی STRIDE را برای طبقه‌بندی تهدیدات امنیتی پیشنهاد کرد [۷].STRIDE مخفف و مشتق شده از شش دسته تهدید زیر است: (۱) جعل هویت، (۲) دستکاری در داده‌ها، (۳) انکار، (۴) افشای اطلاعات، (۵) DoS، و (۶) افزایش امتیاز.

استاندارد ISO 7498-2[۸]، پنج نوع تهدید امنیتی عمده را فهرست کرده‌است: (۱) تخریب اطلاعات و/یا منابع دیگر، (۲) فساد یا اصلاح اطلاعات، (۳) سرقت، حذف یا ازدست دادن طلاعات و/ یا سایر منابع، (۴) افشای طلاعات، و (۵) وقفه در خدمات.

جوینی و همکاران [۹] مدل طبقه‌بندی چند بعدی تهدیدات را مطابق با پنج معیار اساسی زیرپیشنهاد کردند: (۱) منبع تهدید، (۲) عامل تهدید، (۳) انگیزه تهدید، (۴)قصد تهدید و (۵) اثرات تهدید.جوینی و همکاران اثرات تهدیدی زیر را شناسایی کردند:

---

[3]Confidentiality, integrity, and availability
[4]denial of service

تخریب اطلاعات، فساد اطلاعات، سرقت/ از دست دادن اطلاعات، افشای اطلاعات، محرومیت از استفاده، افزایش امتیاز، و استفاده غیرقانونی.

هاوارد و لانگستاف [۱۰] یک طبقه‌بندی امنیتی یکپارچه را در سال ۱۹۹۸ بر اساس تعاریف رویداد، حمله و حادثه پیشنهاد کردند. این طبقه‌بندی تلاش می‌کند تا یک حمله را بر اساس ابزار مورد استفاده، آسیب‌پذیری مورد سوءاستفاده قرارگرفته، اقدام انجام شده، هدف و نتیجه غیرمجاز تعریف کند.

زو و همکاران [۱۱] یک طبقه‌بندی برای حملات سایبری سیستم‌های اسکادا پیشنهاد کردند که تهدیدها را براساس مکان حملات از نظر ظهور و آشکارسازی آنها دسته‌بندی می‌کند. این طبقه بندی چهار دسته حمله زیر را در نظر می‌گیرد: (۱) پیاده‌سازی پروتکلها، (۲) سخت‌افزار، (۳) پشته ارتباطی، و (۴) نرم‌افزار. این طبقه‌بندی جامع نیست و فقط حملات برجسته ICS را هدف قرار می‌دهد.

میلر و همکاران [۱۲، ۱۳] تلاش کردند تا چارچوبی باز و جامع برای طبقه‌بندی حوادث مختلف در سیستم‌های فیزیکی-سایبری ارائه دهد. میلر و همکاران حوادث طبقه‌بندی شده را بر اساس پارامترها و پارامترهای فرعی زیر: (۱) نوع منبع، (۲) میانگین، (۳) تاثیر (تاثیرمستقیم، تاثیرغیرمستقیم، شدت تاثیر، فوری بودن تاثیر، زمان بازیابی و تاثیر پولی) و (۴)) قربانی (نوع قربانی و بخش بازار قربانی). آنها توضیح بسیار مختصری از پنج طبقه‌بندی حملات سایبری یا حوادث [۱۰، ۱۴-۱۷] را به عنوان بررسی ادبیات ارائه کردند.سپس طبقه‌بندی پیشنهادی آنها ارائه می‌شود. میلر و همکاران ارزش PD را در زیر پارامتر ضربه مستقیم برای تجزیه و تحلیل حوادث به معنای تأثیر آنها بر دنیای فیزیکی اضافه کرده‌اند. در زیر بخش ۲.۳، ما این طبقه‌بندی‌ها را درجدول ۱ با هم مقایسه خواهیم‌کرد.

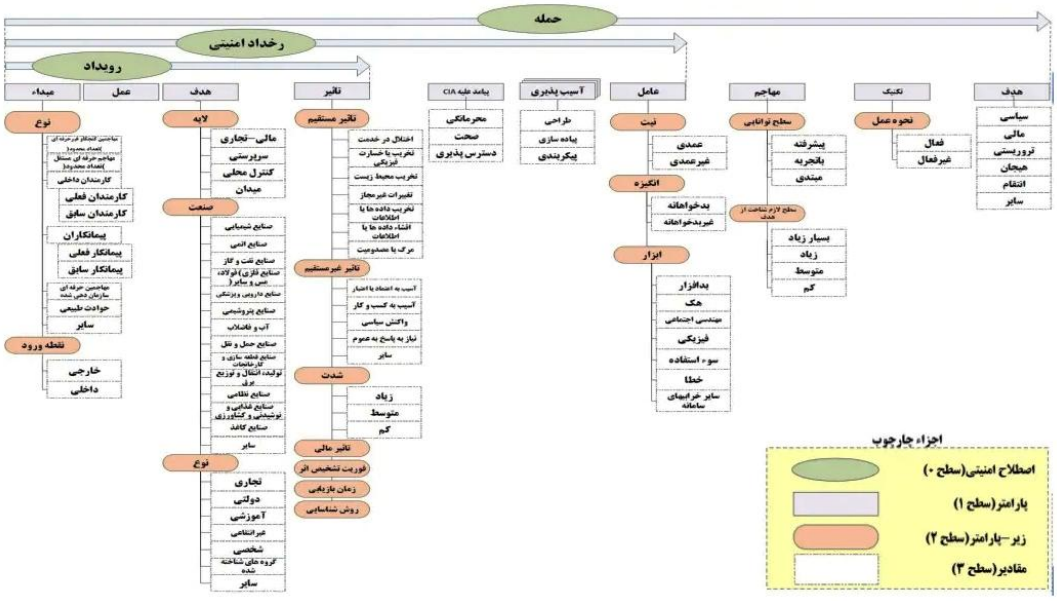
MITER ATT&CK1[5] یک پایگاه دانش و مدلی برای رفتار دشمن سایبری است که منعکس‌کننده مراحل مختلف چرخه زندگی دشمن است. اگرچه ATT&CK برای درک ریسک امنیتی در برابر رفتار دشمن شناخته شده مفیداست، اما برای برنامه‌ریزی به بودهای امنیتی، اهداف آن با HTF متفاوت است.

میلر و رو [۱۸] پانزده حمله امنیت سایبری را که شامل زیرساخت‌های حیاتی و سیستم‌های اسکادا در بازه زمانی ۱۹۸۲ تا ۲۰۱۲ بود، تجزیه و تحلیل کردند. آنها این حوادث را تنها براساس چهار معیار (بخش منبع،روش عملیات،تأثیر و بخش هدف) طبقه‌بندی کردند و تجزیه و تحلیل آماری خود را گزارش کردند. معیار بخش هدف در میلر و رو در [۱۸] منبع حادثه مانند تجاری، دولتی و آموزشی را شناسایی کردند و آن معیار خاصی برای تجزیه و تحلیل ICS نیست. بر خلاف معیارهای کلی که می‌تواند به هر حادثه مرتبط باشد، «معیارهای خاص برای تجزیه و تحلیلICS» معیارهایی هستند که به‌طور ویژه برای مرتبط بودن با ICS و فناوری‌های مربوط به آنها مانند لایه هدفICS و صنعت هدفICS تعریف شده‌اند.

[5]https://attack.mitre.org/

اوجی [۱۹]، ۲۴۲ حادثه امنیتی را در زیرساخت‌های حیاتی و شبکه‌های کنترل صنعتی که بین سال‌های ۱۹۸۲ و ۲۰۱۴ در پایگاه‌داده آنلاین RISI[6] گزارش شده‌اند، تجزیه و تحلیل کرد. آنها این حوادث را تنها براساس چهار معیار (قصد، روش عملیات، ارتکاب به جنایت و بخش هدف) طبقه‌بندی کردند و تجزیه و تحلیل آماری خود را گزارش کردند. معیار بخش هدف در اوجی [۱۹] شبکه‌های زیرساخت حیاتی و انواع ICS شناسایی کرد که در آنها حوادث رخداده است.

احمدیان و همکاران « چارچوب طبقه‌بندی سلسله مراتبی»[7] را در [۲۰] با شانزده ویژگی مورد نیاز برای طبقه‌بندی حملات و حوادث امنیتی در ICS پیشنهاد کردند. در این تحقیق تعاریف نیمه رسمی و استاندارد شده‌ای از تهدیدها، رویدادها، حوادث، غیرحادثه، حوادث غیرامنیتی، حوادث امنیتی غیرحمله‌ای و حملات ارائه کردید. HTF دارای معیارهای قابل توجهی است که اطلاعات را برای هوش تهدیدات دسته‌بندی می‌کند. این چارچوب دارای ویژگی‌های مناسبی مانند کامل بودن، عدم ابهام، تکرارپذیری، مفید بودن، مناسب بودن و کاربردی بودن است. این طبقه‌بندی پیشنهادی با پارامترها و پارامترهای فرعی مختلف، چارچوب سلسله مراتبی قابل گسترش را برای نیازهای هر سازمانی آماده می‌کند. پارامترها و پارامترهای فرعیHTF را می‌توان برای سایر برنامه‌هایی که نیاز به سفارشی سازی بیشتری دارند تغییر، گسترش و اصلاح کرد. در این تحقیق همچنین ۲۶۸ حادثه امنیتی را در ICS طبقه‌بندی و تجزیه و تحلیل‌گردید(شکل ۳)



شکل۳ : چارچوب طبقه‌بندی سلسله مراتبی

۲-۲- مروری بر مفاهیم:

در حوزه امنیت سایبری به کرات شاهد این هستیم که واژگان کلیدی، تهدید(Threat)، رویداد(Event)، حادثه امنیتی(Security Incident)، حادثه امنیتی غیرتهاجمی(Non-Attack Security Incident) و حمله(Attack) به اشتباه به جای یکدیگر به کار می روند. در این بخش،تعاریف اصطلاحات و پارامترهای امنیتی مرتبط را بررسی خواهیم‌کرد.

[6] https://www.risidata.com/Database
[7] Hierarchical Taxonomic Framework (HTF)

۱- تهدید امنیتی[8]:

به‌طور عمومی به مجموعه عواملی در سیستم اطلاق می‌شود که پتانسیل واردکردن آسیب و ضرر به دارایی‌های سیستم را دارند؛ تهدید هر نقض بالقوه امنیت است. البته تعریف تهدید در منابع مختلف با تفاوت‌هایی همراه است به‌عنوان نمونه طبق استاندارد ISO/IEC 13335-1 (2004) و ISO / IEC 27000 (2016)، تهدید به کلیه عوامل بالقوه یک حادثه ناخواسته اطلاق می‌شود که ممکن است با بروز آنها به لطمه دیدن سیستم یا سازمان منجر شود.

طبق استاندارد ANSI/ISA–99 (نسخه جدید آن با عنوان ISA/IEC-62443 ارائه‌شده است) هرگونه رویداد یا عملی که پتانسیل نقض امنیت، ایجاد رخنه و یا واردکردن صدمه را داشته باشد تهدید نامیده می‌شود.

طبق استانداردISA/IEC-62443، اقدام بالقوه آسیب‌رسان (عمدی یا ناخواسته) یا توانایی (داخلی یا خارجی) که تأثیر نامطلوب از طریق آسیب‌پذیری داشته باشد، تهدید نامیده می‌شود.

براساس [۶]، تهدید یک نقض بالقوه امنیت است. در این تحقیق جنبه‌های مختلفی از تعاریف تهدید و حمله را در منابع و استانداردهای مختلف مورد بررسی قرارداده‌ایم. پس از این مطالعه، نتیجه می‌گیریم که نقطه شروع برای طبقه‌بندی حملات،غلبه بر مشکل همپوشانی بین تهدید و حمله است.بیشتر منابع ذکر شده درکارهای مرتبط، بدون توجه به تعریف دقیق این دو مقوله و تفاوت‌های آنها، به تهدیدات و حملات پرداخته‌اند.

در HTF که تعریف را از [۶] انطباق می‌دهد، تهدید یک نقض بالقوه امنیت است. این واقعیت که نقض ممکن است رخ دهد به این معنی است،آن اقداماتی که می‌توانند باعث وقوع آن شوند، باید در برابر آن اتفاق محافظت (یا برای آن آماده) شود. به این اعمال حمله[9]می‌گویند.

برای برآورده ساختن الزامات یک طبقه‌بندی جهت حوادث امنیت سایبری، تعاریف رویداد، حوادث، غیرحوادث، حادثه امنیتی، حادثه امنیتی بدون حمله، و حمله را به عنوان شرایط امنیتیHTF ارائه می‌کنیم. تعاریف پیشنهادی که به عنوا ن سرتیترHTF استفاده شد، در شکل۴ نشان داده شده است. پس از توضیح این اصطلاحات امنیتی، در ادامه این بخش فرعی، هر پارامتر شکل۴ (منبع، اقدام، هدف، تاثیر، نقضCIA، آسیب‌پذیری، عامل، مهاجم، تکنیک عملیاتی، و اهداف) به تفصیل توضیح داده خواهد شد.

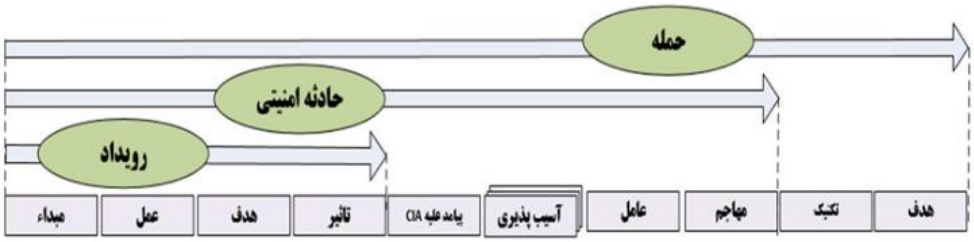
۲- رویداد[10]

دریک مفهوم کلی، یک رویداد تغییرگسسته وضعیت یک سیستم یا دستگاه است [۱۰، ۲۰]. پارامترهای یک رویداد شامل منبع، عمل، هدف و تأثیر رویداد است. درشکل۵، ما اصطلاحات امنیتی اصلی را در یک نمایش بصری سازماندهی می‌کنیم تا تعاریف

---

[8] Security Threat
[9] attacks
[10] Event

دقیق و روابط بین این اصطلاحات را ارائه کنیم. از منظر امنیتی، همانطور که در شکل۵ نشان داده شده است، رویدادها به حوادث و غیرحادثه تقسیم می‌شوند. حوادث به دو دسته حوادث امنیتی و حوادث غیرامنیتی تقسیم می‌شوند.



شکل ۴: سرتیتر HTF

شکل ۵: رویدادها و تعاریف زیرکلاس آن

به هر تغییری از حالت یا وضعیت سیستم را رویداد می‌گوییم. پارامتر رویداد، شامل مبدأ رویداد (مبدأ می‌تواند هرگونه حادثه طبیعی، مهاجمین، کارمندان، پیمانکاران و غیره باشد.)، عمل (که می‌تولند به روش‌های مختلف مقداردهی شود مثلاً مقادیر کاوش، پویش، کپی کردن، تغییر و غیره را برای آن در نظر گرفته است.)، هدف رویداد و تأثیر آن است. همان‌طور که در شکل ذیل مشاهده می‌کنید از زاویه دید امنیتی رویدادها به دو بخش حوادث امنیتی و غیرامنیتی تقسیم می‌شوند. حوادث غیرامنیتی به رویدادهایی نظیر حوادث طبیعی، خرابی تجهیزات و برخی حوادث نظیر انفجار در اثر سهل‌انگاری در انبار کارخانه و افتادن نیرو از ارتفاع گفته می‌شود که در آن‌ها به‌طور قاطع می‌توان اظهارنظر نمود که هیچ موضوع امنیتی مطرح نبوده است.

۲- حوادث

حادثه رویداد یا گروهی از رویدادها است که بر سیستم تأثیر منفی می‌گذارد به نحویکه این تاثیر بر عملکرد،کسب و کار، شهرت و غیره است. به عنوان مثال، یک مهاجم عمدا یا یک کارمند به طور ناخواسته خدمات اصلی یک سیستم را مختل می‌کند.

۳- غیرحادثه

هر رویدادی که در مجموعه حوادث گنجانده نشود، غیرحادثه نامیده می‌شود. غیرحادثه هر تغییری در حین کارکرد عادی یک سیستم است که سیستم را از یک حالت امن به حالت امن دیگر منتقل می‌کند. هیچ نقض خط مشی در طول این تغییر اتفاق نمی‌افتد. مانند ACL یک روتر به روز می‌شود، یا یک خط مشی فایروال تحت فشار قرار می‌گیرد.

۴- حوادث امنیتی

حادثه امنیتی رویدادی است که توسط عامل (عامل‌هایی) عامدانه یا سهوی، بدخواهانه(Malicious) یا غیربدخواهانه انجام‌شده است و تأثیرات آن موجب نقض حداقل یکی از سه اصل محرمانگی(Confidentiality)، صحت(Integrity) و دسترس‌پذیری(Availability) داده یا خدماتشده و این حادثه طبیعتاً می‌تواند ریشه‌ای در یک یا چند آسیب‌پذیری داشته باشد.

۵- حوادث غیر امنیتی

هر حادثه‌ای را که یک حادثه امنیتی نباشد در زمره حوادث غیرامنیتی دسته‌بندی می‌کنیم. این حوادث به هیچ موضوع امنیتی مربوط نمی‌شود.چند نمونه از حوادث غیرامنیتی عبارتند از:

حوادث طبیعی: هنگامیکه یک حادثه طبیعی مانند زلزله رخ می‌دهد، مشخص است که علت حادثه نقص امنیتی نیست و یک هکر یا یک کارمند ناراضی نمی‌تواند این نوع حادثه را ایجاد کند.

خرابی تجهیزات:در بسیاری از موارد، خرابی تجهیزات به طور طبیعی و بناچار در نتیجه فرسودگی یا پیری طبیعی رخ می‌دهد.در مواردی که خرابی تجهیزات منشأ امنیتی نداشته باشد، یک حادثه غیرامنیتی محسوب می‌شود.

تخریب دیوار ساختمان در کارخانه:زمانی که باران یا طوفان شدید، دیوار کارخانه را به دلیل کهنگی فرومی‌ریزد، منشأ امنیتی ندارد و یک حادثه غیرامنیتی محسوب می‌شود.

انفجار در انبار به دلیل سهل‌انگاری:اگر ثابت شود انفجار در یک صنعت ناشی از سهل‌انگاری کارگران یا مهندسان باشد، قطعاً یک حادثه غیرامنیتی محسوب می‌شود.

سقوط کارگر از ارتفاع:در این نوع حوادث مشخص است که هیچ یک از اصول امنیتی سازمان CIA نقض نشده است و این حادثه یک حادثه غیرامنیتی محسوب می‌شود.

۶- حوادث امنیتی غیرتهاجمی

حوادث امنیتی غیرتهاجمی توسط عاملی تحقق می‌یابند که قصد بدخواهانه و عمدی ندارد؛ این عامل می‌تواند یک کارمند ناآگاه یا پیمانکار بی‌توجه باشد. قابل‌توجه است که در برخی موارد می‌تواند مبدأ یک رویداد حادثه‌ای طبیعی باشد اما چنانچه به هر نحوی ما از زاویه‌ی امنیتی به آن بنگریم و تأثیری بر روی هر یک از این سه اصل امنیتی بگذارد، در این تعریف ما آن را حادثه امنیتی غیرتهاجمی در نظر می‌گیریم.

۷- حملات

این نوع حادثه امنیتی با نیت مخرب و اهداف خاص با استفاده از تکنیک‌های عملیاتی اتفاق می‌افتد. در تعریف ارائه شده، هر حمله یک حادثه امنیتی است و هرحادثه امنیتی یک رویداد است، اما عکس این موضوع صادق نیست.رابطه بین این تعاریف در زیر مشخص شده است:

$$Attacks \subset Security\ Incidents \subset Incidents \subset Events$$

$$NonAttackSecurityIncidents \subset Security\ Incidents \subset Incidents \subset Events$$

حمله[11]: حمله نوعی حادثه امنیتی است که به شکل عمدی و بدخواهانه با تکنیک‌ها و اهدافی مشخص انجام‌شده است. بر اساس این زیرساخت تعریفی، هر حمله نوعی حادثه امنیتی و هر حادثه امنیتی یک رویداد است اما عکس آن صحیح نیست.

طبقه‌بندی تهدیدات، حملات و حوادث امنیتی، به سازمان ها، دولت ها و افراد و کارشناسان اجازه می‌دهد تا تهدیدات امنیتی را به‌صورت مشخص شناسایی و مورد بررسی قرار دهند و متناسب با هر تهدید بتواند حملات پیش رو و آسیب‌پذیری‌های مرتبط را مورد تحلیل و موشکافی قرار دهند. آنها بر این اساس می‌توانند تا حد بسیار قابل توجهی منشأ تهدیدات حملات و حوادث و در نتیجه عوامل تأثیرگذار بر آنها را شناسایی نمایند و در نتیجه بر اساس میزان اهمیت منابع مورد تهدید و حساسیت آنها و میران خساراتی که برآورد می‌شود شاخص‌های متعدد مفیدی از جمله شاخص تحلیل مخاطرات را محاسبه نماید.

منبع پارامتر منبع توضیح می‌دهد که یک رویداد کجا و توسط چه عاملی آغاز شده است.منبع یک رویداد می‌تواند رویدادهای طبیعی، مهاجمان، کارکنان، پیمانکاران و غیره باشد.

عمل: براساس فرهنگ لغت استاندارد IEEE اصطلاحات الکتریکی و الکترونیکی، عمل اقدامی است که به سمت هدف انجام می‌شود بطوریکه منجر به تغییرحالت (وضعیت) هدف شود. عمل می‌تواند کاوش، اسکن، کپی، اصلاح و غیره باشد. طبق گفته هاوارد و لانگستاف در [۱۰]، اقدام کاربر مرحله‌ای است برای دست‌یابی به نتیجه‌ای مانند بررسی، اسکن، سیل، احراز هویت، دورزدن، جعل، خواندن، کپی‌کردن، سرقت، تغییر، یا حذف.

هدف: طبق گفته هاوارد و لانگستاف [۱۰]، یک هدف می‌تواند یک کامپیوتر یا یک موجودیت منطقی شبکه (حساب، فرایند یا داده) یا یک موجود فیزیکی (کامپوننت، شبکه یا اینترنت) باشد. در این مطالعه، هدف محدود به دارایی‌های ICS است.

تأثیر: یک حادثه بر سیستم ICS تأثیر منفی می‌گذارد. تأثیر حادثه، خسارت احتمالی است که از حادثه وارد می‌شود و به تأثیرات مستقیم و غیرمستقیم تقسیم می‌شود. ما تأثیرات حادثه را با هفت زیر پارامتر نشان می‌دهیم: تأثیر مستقیم، تأثیر غیرمستقیم، شدت، تأثیر پولی، فوریت تأثیر، زمان بازیابی و روش کشف. تأثیرات مستقیم یک حادثه معمولاً آنهایی هستند که به راحتی قابل مشاهده هستند [۱۳]. این تأثیرات نیز به راحتی قابل درک و اندازه‌گیری هستند. آنها معمولاً بلافاصله یا در مدت کوتاهی پس از حادثه کشف می‌شوند. تأثیرات غیرمستقیم پیامدهای ثانویه یک حادثه هستند و تعیین کمیت آنها دشوارتر است [۱۳]. وقتی این اثرات غیرمستقیم با هم ترکیب شوند، هزینه‌های یک حادثه به طور قابل توجهی افزایش می‌یابد. تأثیر پولی یک رویداد، معیاری از هزینه حادثه برای قربانی است [۱۳]. بی‌درنگ تاثیر یک رویداد، نشان‌دهنده مدت زمانی است که پس از وقوع یک حادثه، تشخیص آن تاثیر طول می‌کشد [۱۳]. زمان بازیابی یک رویداد یکی دیگر از اصلاح کننده‌های تأثیراست [۱۳].

روش کشف : روش کشف نحوه کشف یک رویداد را تعیین می‌کند. روش‌های کشف موجود عبارتند از: سرویس نظارت، پاسخ به حادثه، ممیزی و غیره.

[11] Attack

نقض CIA: اصل امنیتی CIA (سه‌گانه CIA) شامل محرمانگی، صداقت و دردسترس بودن است. سه سرویس کلیدی که باید در هر سیستم ایمن تضمین شود. پارامترنقض CIA نشان می‌دهدکه کدام اصل امنیتی در یک حادثه امنیتی نقض شده است.

آسیب‌پذیری: طبق استاندارد IETF RFC 2828 آسیب‌پذیری یک ضعف در طراحی یا مشخصات، پیاده‌سازی، یا عملیات و مدیریت (پیکربندی) سیستم است که می‌تواند برای نقض خط مشی امنیتی سیستم مورد سوء استفاده قرار گیرد[۱۰]. در هر حادثه امنیتی،یک آسیب‌پذیری یا گروهی از آسیب‌پذیری‌ها می‌تواند مورد سوء استفاده قرارگیرد.

عامل: شخص یا چیزی که نقش فعالی را ایفا می‌کند یا اثر مشخصی را در یک حادثه ایجاد می‌کند. هنگامی‌که آسیب‌پذیری‌ها در یک سیستم وجود داشته باشد، یک حادثه امنیتی ممکن است از طریق یک عامل حادثه امنیتی با استفاده از یک ابزار خاص برای ایجاد اثرات نامطلوب (به عنوان مثال،نقض خط‌مشی) آشکارشود. هر عاملی قصد و انگیزهای دارد.قصد عامل نشاندهنده قصد عاملی است که باعث حادثه شده‌است [۹]. مامور معمولاً انگیزه خاصی برای سازماندهی یک حادثه امنیتی دارد. این انگیزه‌ها می‌توانند مخرب یا غیرمخرب باشند.

مهاجم: مهاجم عاملی است که برای دستیابی به یک هدف خاص به یک سیستم با نیت مخرب حمله می‌کند.

تکنیک عملیاتی: تکنیک‌های عملیاتی تعیین می‌کنند که مهاجمان از چه روش‌هایی برای رسیدن به اهداف خود استفاده می‌کنند. یک حمله می‌تواند شامل چندین تکنیک عملیاتی باشد.

اهداف: طبق گفته هاوارد و لانگستاف [۱۰]، اهداف حمله، اهداف یا اهداف نهایی یک حمله هستند.

۳– بررسی حوادث امنیتی منتخب :

در این تحقیق، مهمترین حوادث ICS دردسترس عموم را جمع‌آوری کردیم. برای دستیابی به این هدف، برجسته‌ترین منابع رویداد ICS مانند ICS-Cert[12]، Bitdefender، Symantec، Securelist، Securityweek، Computerworld، پایگاه داده آنلاین مخزن حوادث امنیت صنعتی (RISI[13])، آزمایشگاه ملی آیداهو[۱۴] و برخی از مقالات را بررسی و تحلیل کردیم. به عنوان مثال [۱۸] و [۱۹]. مجموعه داده شامل ۲۶۸رویداد امنیتی ICS است که به طور عمومی گزارش شده است که بر کنترل فرایند یا اتوماسیون صنعتی در سیستم‌های SCADA یا DCS در بازه زمانی سالهای ۱۹۸۲ تا ۲۰۱۸ تأثیر گذاشته است. در مجموعه داده جمع‌آوری شده، پنج مورد از علائم ترافیک و رویدادهای بیمارستانی RISI[۲۸-۳۲] را که غیرمرتبط باICS بودند، حذف کردیم.

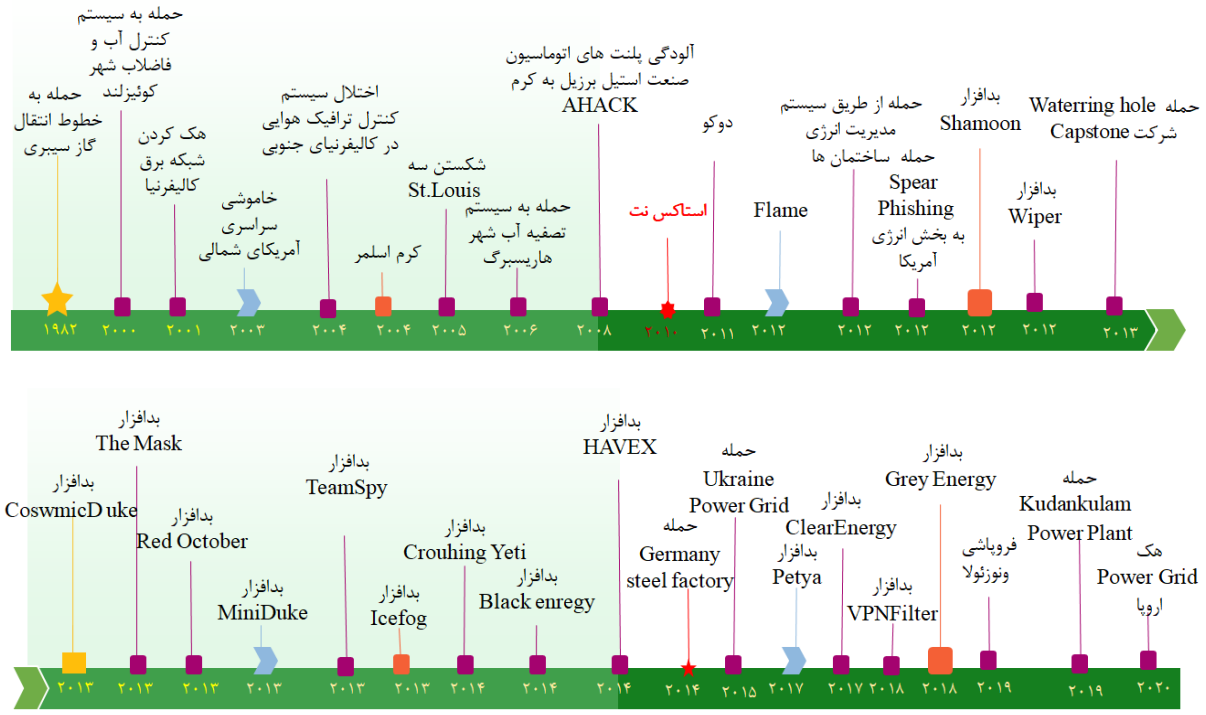
در فرایند طبقه‌بندی حوادث امنیتی، اطلاعات مربوطه را جمع‌آوری کردیم و سپس مقادیر پارامترها و زیر پارامترها را مطابق چارچوب پیشنهادی تکمیل کردیم. در ادامه این بخش، ابتدا در جدول۱، برخی از کارهای مرتبط در زمینه حوادث امنیتی ICS را

[12] https://ics-cert.us-cert.gov
[13] http://www.risidata.com
[14] https://www.inl.gov

که در بخش فرعی ۲.۱ بررسی شده است، مقایسه می‌کنیم.پس از آن، به دلیل محدودیت فضا، تنها ۱۶ حادثه امنیتی برجسته ICS را به ترتیب زمانی به طور خلاصه شرح می‌دهیم(شکل۶).

جدول ۱: ویژگی‌های کار مرتبط

	[۱۸]	[۱۹]	[۲۰]
سال انتشار	۲۰۱۲	۲۰۱۷	۲۰۱۹
تعداد حوادث	۱۵	۲۴۲	۲۶۸
دوره زمانی پوشش داده شده	۱۹۸۲ تا ۲۰۱۲	۱۹۸۲ تا ۲۰۱۴	۱۹۸۲ تا ۲۰۱۸
انواع حوادث	فقط حملات	حملات و حوادث امنیتی	حملات و حوادث امنیتی
تعداد معیارهای تجزیه و تحلیل	۴	۴	۲۲
معیارهای خاص برای تجزیه و تحلیل ICS		یک معیار	دو معیار
منابع	۱۰ منبع متفاوت	فقط پایگاه داده آنلاین RISI	بیش از ۲۰ منبع متفاوت



شکل ۶: حملات و هم حوادث امنیتی

این حوادث نماینده مهمترین حوادث امنیتی در ICS و زیرساختهای حیاتی در شرایط مختلف هستند. ما اطلاعات هر یک از این رویدادها را بر اساس چارچوب پیشنهادی در جدول۲ لیست کرده‌ایم تا نشان‌دهیم که چگونه می‌توان از HTF پیشنهادی با

مثال‌های واقعی استفاده کرد.درجدول۱، ستونی که با [۲۰] مشخص شده است، ویژگی‌هایHTF را نشان می‌دهد.که هم حملات و هم حوادث امنیتی را در نظر گرفت.

اوجی [۱۹] نیز هم حملات و هم حوادث امنیتی را در نظرگرفت، اما میلر و رو [۱۸] فقط حملات را درنظر گرفتند. ما از بیست و دو معیار برای تجزیه و تحلیل حوادث استفاده کردیم اما اوجی [۱۹]و میلر و رو [۱۸] تنها از چهار معیار استفاده کردند. ما از معیارهای خاصی برای تجزیه و تحلیل ICS در HTF مانند لایه هدف ICS و صنعت هدف استفاده کردیم، اما همانطور که در بخش ۲ توضیح دادیم، میلر و رو [۱۸] از هیچ معیار خاصی برای تجزیه و تحلیل ICS استفاده نکردند. اوجی [۱۹] از بخش هدف به عنوان یک معیار خاص برای تجزیه و تحلیل ICS برای شناسایی زیرساخت‌های حیاتی و انواع ICS استفاده کرد که در آن حوادث رخداده است.

۱-۳- سیستم آبی ماروچی (۲۰۰۰)

در مارس ۲۰۰۰، ماروچی شیر در کوئینزلند مشکلاتی را در سیستم فاضلاب جدید خود تجربه کرد. ارتباطات ارسال شده از طریق لینکهای رادیویی به ایستگاههای پمپاژ فاضلاب از بین می‌رفت، پمپ‌ها به درستی کار نمی‌کردند و آلارم‌های نصب شده برای هشدار به کارکنان خاموش نمی‌شد. ابتدا فکر می‌کردند مشکل به دلیل سیستم جدید است اما پس از مدتی متوجه هک شدن سیستم شدند.شخصی به نام"بودن[۱۵]" توانست ۱۵۰ ایستگاه پمپاژ فاضلاب را با استفاده از لپ تاپ و فرستنده رادیویی کنترل کند. او در مدت سه ماه، یک میلیون لیتر فاضلاب تصفیه نشده را در یک زه کشی آب رها کرد وا ز آنجا به آبراه‌های محلی سرازیر شد. این حمله انتقام او پس از این که نتوانست شغل خود را حفظ کند بود.

۲-۳- سرایت ویروسی شبیه ساز آموزشی اپراتور نفت (۲۰۰۲)

درسال ۲۰۰۲، یک شبیه ساز آموزش اپراتور به سایتی از کارخانه‌ای در هیوستون ارسال شد. قبل از اتصال سیستم DCS آموزشی، با روشی استاندارد چک کردن سیستم، تشخیص دادند که شبیه‌ساز به یک ویروس کامپیوتری رایج آلوده شده است. بعید بود که این ویروس هیچ تاثیر مستقیمی بر عملیات فرایند داشته باشد، زیرا سیستم آموزشی به سیستم‌های فرایند بلادرنگ متصل نشده بود.

۳-۳- نیروگاه هسته‌ای دیویس بیس (۲۰۰۳)

در ژانویه ۲۰۰۳، کرم SQL Slammer نیروگاه هسته‌ای اوهایو را آلوده کرد. این کرم باعث شد یک سیستم نظارتی حدود ۵ ساعت کار کند و بیش از ۶ ساعت طول کشید تا سیستم به حالت عادی برگردد. اسلمر توانسته است بیش از ۹۰ درصد از سیستمهای آسیب‌پذیر جهان را در کمتر از پنج دقیقه آلوده کند. کرمSlammer از آسیب‌پذیری سرریز بافر استفاده کرد. هنگامی که کرم یک

[15] Boden

سیستم را آلوده کرد، سپس رایانه آلوده، شبکه را اسکن کرد تا رایانه‌های آسیب‌پذیر دیگری را در پورت ۱۴۳۴ ، آدرس‌های دلخواهی را پیدا کند.

۴-۳- سد سن لوئیس (۲۰۰۵)

در دسامبر ۲۰۰۵، یک خطای اندازه‌گیری در یک سیستم کنترلی در سد سنت لوئیس در میسوری باعث شکست بزرگ در سد شد. سد شکسته شد و مردم در منطقه‌ای به قطر ۴ مایل در معرض خطر بودند. در این حادثه خسارات اقتصادی زیادی به زمین‌های کشاورزی وارد شد. لایه هدف این حادثه شبکه میدانی بود.

۵-۳- هک TCCA[16] (۲۰۰۷)

یک کارمند سابق یک سیستم کانال کوچک درکالیفرنیا، روزی که پس از ۱۷ سال کار در شرکت اخراج شد. نرم‌افزار غیرمجاز را روی سیستم اسکادای TCCA نصب کرد. چنین حملاتی از این جهت مهم هستند که توسط کارکنان داخلی، افرادی که اجازه دسترسی به بخش‌های مختلف شبکه‌ها را دارند، انجام می‌شوند. بنابراین، حتی اگر این شبکه‌ها کاملاً ایزوله باشند، باز هم ممکن است توسط افراد داخل سازمان مورد حمله قرار گیرند.

۶-۳- عفونت کارخانه فولاد با کرم Ahack (۲۰۰۸)

در سال ۲۰۰۸، در برزیل، یک پیمانکار سابق که از طریق اینترنت به داخل یک کارخانه فولاد دسترسی داشت، کرمی به نام Ahack را در کارخانه برق و کوره بلند این شرکت منتشر کرد. این کرم در سراسر شبکه اتوماسیون پخش شد، خسارات مالی زیادی به بارآورد و ارتباطات بین PLC و ایستگاههای نظارت را مختل کرد. طغیان بسته‌های ناخواسته ارتباط بین PLCها و ایستگاه‌های نظارتی را ناپایدار کرد و منجر به از دست‌دادن دید شد. از دست‌دادن دید، باعث توقف و راه‌اندازی مجدد سیستم‌های اسکادا شد. این کرم همچنین برخی از سیستم‌های دارای سیستم عامل ویندوز را مختل کرد.

۷-۳- حمله استاکس‌نت به تاسیسات هسته‌ای ایران (۲۰۱۰)

استاکس‌نت اولین بدافزار بسیار پیچیده بود. این اولین کرم کشف‌شده‌ای است که سیستم‌های صنعتی را جاسوسی و برنامه‌ریزی مجدد می‌کند و اولین کرمی است که یک روت‌کیت[17] PLC را شامل می‌شود. هدف گمانه‌زنی‌شده، خرابکاری در برنامه هسته‌ای ایران و به‌طورمشخص‌تر، کارخانه غنی‌سازی اورانیوم نطنز بود. پس از آلوده‌کردن چنین سیستم‌هایی، استاکس‌نت PLCها را مجدداً برنامه‌ریزی می‌کند تا سانتریفیوژها را با سرعتی خارج از حد مجاز کارکند. روش آلودگی اولیه مشخص نشده‌است، اما با توجه به اینکه سیستم‌هایPLC معمولاً به اینترنت متصل نیستند، می‌تواند به دلیل استفاده از درایو متحرک آلوده باشد. استاکس‌نت کد روت‌کیت را برای مخفی کردن باینری‌های خود در سیستم‌های ویندوز و همچنین کد PLC را برای ارائه مقادیر قابل قبول به

[16] Tehama Colusa Canal Authority
[17] Rootkit (مجموعه‌ای از ابزارهای نرم‌افزاری که به کاربر غیرمجاز اجازه می‌دهد تا کنترل یک سیستم کامپیوتری را بدون شناسایی شدن به دست آورد)

نرم‌افزار نظارت تغییرداد، اگرچه سیستم‌های واقعی بالاتر از حد مجاز کار می‌کردند . همچنین از دو گواهی دیجیتال در معرض خطر برای امضای درایورهای خود در تلاشی بیشتر برای فرار از تشخیص استفاده‌کرد.

محصولات امنیتی شناخته‌شده نقطه پایانی را اسکن کردند و براساس نام و نسخه محصول، اطلاعات یا پیام واقعی در داده‌های ارسالی، آن را تزریق کرد. یکی از ویژگی‌های جالب بدافزار این بود که تاریخچه ماشین‌های آلوده، از جمله نام دامنه و آدرسIP آنها را حفظ می‌کرد. استفاده از روت‌کیت PLC، تکنیک‌های پیچیده فرار از آنتی‌ویروس، تزریق فرایند پیچیده، و قلاب کردن کد و به‌روزرسانی‌های همتا به همتا، استاکس‌نت را به یکی از پیچیده‌ترین حملات مشاهده شده تا به امروز تبدیل کرده است.

۸-۳- دوکو[18] (۲۰۱۱)

حمله دوکو در سپتامبر ۲۰۱۱ شناسایی شد.با این‌حال، اعتقاد براین است که از فوریه ۲۰۱۰ فعال بوده و از سال ۲۰۱۲ غیرفعال است. دوکویک تروجان است و به‌نظرمی‌رسد که توسط همان افرادی طراحی شده‌است که استاکس‌نت را ایجاد کرده‌اند، اما برخلاف استاکس‌نت که خرابکاریهای صنعتی را انجام می‌دهد،دوکو برای سرقت اطلاعات مربوط به نصب ICS ها طراحی شده‌است. تفاوت دیگر این است که دوکو خودتکراری با سیستم‌های دیگری مانند استاکسنت نمی‌کند. مهاجمان از ایمیل هدفمند با سند مایکروسافت ورد باسوء استفاده از هسته روزصفر[19] استفاده کردند که دوکو را روی سیستم هدف نصب کردند. این آسیب‌پذیری به مهاجمان اجازه می‌دهد تا کدهایی با بالاترین سطح امتیاز اجرا کنند و مکانیسم‌های امنیتی را دور بزنند. دوکو می‌تواند پس از ۳۰ روز خود را حذف کند. علاوه براین، اگر مهاجمان کشف می‌شدند یا کنترل سیستم‌های در معرض خطر را از دست می‌دادند، بدافزار درنهایت خود را به‌طورخودکارحذف می‌کند تا از کشف احتمالی جلوگیری کند.

در این حمله پیچیده سطح بالا از سه آسیب‌پذیری اصلاح نشده استفاده شده است. برای پنهان ماندن این حمله، بدافزار تنها در حافظه kernel مقیم شده است در نتیجه راه حل‌های ضد بدافزاری قادر به تشخیص آن نیستند. این بدافزار برای گرفتن دستورات مستقیما به یک سرور C&C متصل نشده است بلکه مهاجم فایروال‌ها و دروازه‌های ورودی شبکه را با نصب درایوهای مخرب آلوده کرده و در نتیجه تمامی ترافیک شبکه خارجی به سرورهای C&C مهاجم از طریق پروکسی منتقل شده است.

به نظر می رسد که بدافزار دوکوسال ۲۰۱۱ با دوکوسال ۲۰۱۵ در ارتباط است زیرا هر دو حاوی کدهای مشترک زیادی هستند.شرکت سایمانتک اعلام کرد که دوکونسخه ۲.۰ یک ابزار سرقت اطلاعات با ویژگی‌های کامل است که برای استفاده در دراز مدت طراحی شده است. به احتمال زیاد سازندگان این بدافزار از آن به عنوان یکی از ابزارهای اصلی خود در کمپین‌های هوشمند جمع‌آوری اطلاعات استفاده می‌کنند.

۹-۳- شامون (۲۰۱۲)

[18]Duqu
[19]zeroday

شامون[۲۰] از خانواده بدافزار تهاجمی و بسیار مخرب است که با پاک کردن ماشین‌های قربانی درسال ۲۰۱۲ علیه بخش انرژی آرامکو عربستان سعودی استفاده شد. این حمله باعث خرابی فایل‌ها در یک کامپیوتر در معرض خطر شد و MBR[۲۱] را بازنویسی کرد. از اجزای متعددی مانند Dropper، Wiper و Reporter تشکیل شده‌است.

۱۰-۳- شعله (۲۰۱۲)

شعله[۲۲] یک کرم جاسوسی سایبری است که تعداد زیادی از کشورهای خاورمیانه، اروپا و آمریکای‌شمالی را آلوده کرده‌است. این بدافزار بزرگترین جاسوسی سایبری کشف شده تا سال۲۰۱۲ و یکی از پیچیده‌ترین تهدیداتی بود که تاکنون کشف شده‌است.. اندازه کلی ماژول‌ها ۲۰ مگا بایت است زیرا از کتابخانه‌های زیادی برای فشرده‌سازی و دستکاری پایگاه‌داده استفاده می‌کند. برخی از قابلیت‌ها عبارتند از: شنود ترافیک شبکه، گرفتن اسکرین‌شات، ضبط مکالمات صوتی، رهگیری صفحه‌کلید و غیره. ابزار انتشار کابل‌های USB و LAN هستند.

۱۱-۳- وایپر (۲۰۱۲)

وایپر[۲۳] بدافزاری است که در سال ۲۰۱۲ به شرکت‌های انرژی، نفت و گاز و نهادهای دولتی در ایران حمله کرد. هدف این حمله ازبین بردن نیمه اول دیسک و سپس پاک کردن فایل‌های مهمی بود که برای عملکرد صحیح سیستم موردنیاز بودند و این فرایند منجر به از کارافتادن سیستم مورد حمله می‌شد. مهاجمان بسیار مراقب بودند که تمام داده‌هایی را که می‌توان برای ردیابی آنها استفاده‌کرد، از بین ببرند و به همین دلیل، شاید هیچ‌کسی هرگز متوجه نشد که وایپر دقیقاً چه بوده‌است. فایلهای سیستم آلوده قابل بازیابی نبودند و سیستم‌عامل پس از نصب مجدد آن بارگذاری نمی‌شد زیرا وظایف فقط تا مرحله بارگذاری BIOS انجام می‌شد. انتشار وایپر ازطریق USB و منابع مشترک در شبکه‌ها بود.

۱۲-۳- هاوکس (۲۰۱۴)

Oldrea که با نام هاوکس[۲۴] یا Energetic Bear شناخته می‌شود، یک درب پشتی در رایانه قربانی است که به مهاجمان اجازه می‌دهد داده‌ها را استخراج کنند یا بدافزار دیگری را نصب کنند. علاوه براین، هاوکس یک تروجان دسترسی از راه‌دور (RAT[۲۵]) است که با یک سرور فرمان و کنترل (C&C[26]) ارتباط برقرارمی‌کند. کاربرد اصلی Havex Loder دانلود و بارگذاری ماژولهای DLL اضافی در حافظه است. این DLLها در وبسایت‌های در معرض خطر که به عنوان سرور C&C عمل می‌کنند استفاده می‌شوند. بدافزار

---

[20]Shamoon
[21]Master Boot Record
[22]Flame
[23]Wiper
[24]Havex
[25]Remote Access Trojan
[26]command andcontrol

از طریق فیشینگ، ایمیل‌های هرزنامه، و وب‌سایت‌ها از طریق حملات گودال آب[27]درحال گسترش است. هاوکس از استاندارد ارتباطات پروتکل باز (OPC[28])که یک پروتکل معمولی ICS است استفاده کرده است. این پروتکل بهترین انتخاب برای انتقال اطلاعات بدون احرازهویت، منبع یا داده است. هاوکس مستقیماً پروتکل را هدف قرار نداده‌است، اما شاید اطلاعاتی را برای مرحله دیگری از حمله جمع‌آوری کرده‌است. همچنین می‌تواند نرم‌افزار ICS را آلوده‌کند و در نتیجه می‌تواند سدهای برق آبی را غیرفعال کند، نیروگاه‌های هسته‌ای را بیش از حد بارگذاری کند، و حتی می‌تواند شبکه برق یک کشور را خاموش کند.

۱۳-۳- کارخانه فولاد آلمان (۲۰۱۴)

در سال ۲۰۱۴، مهاجمان به یک کارخانه فولاد در آلمان نفوذ کردند. مهاجمان از طریق ایمیل فیشینگ به یک شبکه کارخانه منتقل شدند.فیشینگ به مهاجمان کمک کرد تا به شبکه و سیستم‌های تولید دفتر کارخانه دسترسی پیدا کنند.مهاجمان دانش خوبی از کنترل‌های صنعتی کاربردی و فرایندهای تولید سیستم هدف داشتند و آسیب فیزیکی زیادی به سیستم وارد کردند.گزارش قابل اعتمادی وجود ندارد که تأیید کند این حمله یک APT بوده‌است.ایمیل‌ها احتمالاً حاوی PDF مخربی بودند که باعث دانلود و اجرای یک کد مخرب شده‌است. دلیل خسارات عظیم این بود که کارخانه قادر به خاموش کردن کوره بلند به روشی منظم نبود.

۱۴-۳- Industroyer (۲۰۱۶)

Industroyer که با نام Crash Override نیز شناخته می‌شود، یک پلتفرم حمله ماژولار ICS بسیار توانمند است که طبق گزارش‌ها در سال ۲۰۱۶ علیه زیرساخت‌های حیاتی اوکراین مورد استفاده قرار گرفت. این بدافزار روی سازمان‌هایی که از پروتکل‌های ICS:IEC101،IEC104، OPC DA و IEC61850 استفاده می‌کنند، متمرکز شده‌است.چندین قابلیت گزارش شده Industroyer ازجمله صدور دستورات معتبر به RTU ها، حملهDoS به پورت‌های COM سریال محلی در دستگاه‌های ویندوز، اسکن و نقشه‌برداری از محیط ICS، و بهره‌برداری از آسیبپذیریDoS رله زیمنس است.

Industroyer دومین بدافزاری است که بدون نیاز به مداخله نفوذگران، این امکان را فراهم می‌کند تا با دسترسی به سیستم‌های آلوده، فرایندهای تجاری و صنعتی را مختل کند. پیش از این استاکس نت در سال ۲۰۱۰ میلادی توسط ایالات متحده آمریکا و رژیم غاصب صهیونیستی با هدف حمله به برنامه‌های اتمی ایران توسعه یافته بود.

۱۵-۳- باج‌افزار ClearEenergy (۲۰۱۷)

ClearEnergy یک باج‌افزار است که زیرساخت‌های حیاتی و سیستمهای اسکادا مانند نیروگاه‌های هسته‌ای و نیروگاه‌ها، تاسیسات آب و زباله و غیره را هدف قرار می‌دهد. این بدافزار براساس خطرناک‌ترین آسیب‌پذیری موجود در سیستمهای اسکادا و ICS است و

[27]watering hole attacks
[28]Open Protocol Communications

به همین دلیل می‌تواند طیف گســـترده‌ای از تولیدکنندگان و فروشـــندگان را تحت تاثیر قراردهد. پس از اجرای بدافزار، PLCهای آسیب پذیر را جستجو می‌کند تا نمودارهای منطقی پلکانی را از PLC بگیرد و آنرا به یک سرور راه‌دور ارسال کند. سپس، یک تایمر شروع به راه‌اندازی فرایندی برای پاک کردن نمودار منطقیPLC می‌کند.

تنها درصـــورتی لغو می‌شـــود که قربانی باج درخواســـتی را پرداخت کند. ClearEnergy از یک نقص امنیتی در پروتکلUMAS تامین‌کننده اشـنایدرالکتریک به علت طراحی بد کلید جلسـه که باعث دور زدن احراز هویت می‌شـود اسـتفاده می‌کند. با اسـتفاده از این نقص، مهاجم می‌تواند کلید جلسه یک بایتی را حدس بزند یا آنرا بشـنود و کنترل کامل کنترلرها را در اختیار بگیرد. هنگامیکه مهاجم یک کلید جلســه متن شـفاف را به دســت‌آورد، می‌تواند درخواســت را دوباره پخش‌کند، دســتورات دلخواه از جمله توقف و راه‌اندازی PLC را اضافه کند و نمودار پلکانی آنرا دانلود کند.

۱۶-۳- تریتون (۲۰۱۷)

تریتون[۲۹] که به عنوان Trisis نیز شـناخته می‌شود، اولین بدافزار شـناخته شده علیه سیسـتم ابزارایمنی (SIS) ICS است. تریتون یک چارچوب حمله است که برای تعامل با کنترلرهایTriconex SIS ساخته شده است. درسال ۲۰۱۷، مهاجمان به یک ایستگاه کاری مهندسی SIS از راه‌دور دسترسی پیدا کردند و چارچوب حمله تریتون را برای برنامه‌ریزی مجدد کنترل‌کننده‌های SIS به‌کارگرفتند. اعتقاد براین اســـت که مهاجمان درســـناریوی خود از حمله زنجیره تامین اســـتفاده‌کردند. این بدافزار با چندین ویژگی ســـاخته شـده‌اسـت، از جمله توانایی خواندن و نوشـتن برنامه‌ها، خواندن و نوشـتن عملکردهای فردی، و پرس و جو از وضـعیت کنترلر SIS. برخی از مطالعات نشـان می‌دهد که مهاجمان اطلاعات دقیقی از پروتکل اختصـاصـی TriStation داشـتند که به‌طور عمومی مسـتند نشده است.

در جدول ۲، ما ۱۶ رویداد ICS را با اسـتفاده از HTF طبقه‌بندی می‌کنیم تا نشـان دهیم که چگونه می‌توان از چارچوب با مثال‌های واقعی اســـتفاده کرد. در آنالیز، دو پارامتر دیگر را اضـــافه می‌کنیم که به آنها اعتبار اطلاعات و مقدار اطلاعات فنی قابل دســـترس می‌گویند. با توجه به فضـــای محدود جدول، مقادیر پارامترها و زیر پارامترها با اختصـــاراتی که در جدول ۳ تعریف شـــده اســـت پر شده‌است.

[29] Triton

جدول ۲: خلاصه ۱۶ رخداد ICS منتخب

حادثه امنیتی	سال	مکان	اعتبار	مقدار اطلاعات	منبع / نقطه ورود	منبع / نوع	هدف / لایه	هدف / صنعت	هدف / نوع	تاثیر / مستقیم	تاثیر / غیرمستقیم	نقض CIA	عامل / قصد	عامل / انگیزه	عامل / وسیله	عامل / قابلیت	عامل / سطح شناسایی هدف	عملیات	تکنیک / مد هدف
سیستم آبی ماروچی	۲۰۰۰	استرالیا	تائید شده	برخی از جزئیات	داخلی	پیمانکاران سابق	LC,FN	صنعت آب و فاضلاب	دولتی	DS,ID SD	LR, PoR, PuR	A, I	عمدی	مخرب	استفاده نادرست از منابع	پیشرفته	خیلی‌زیاد	فعال	انتقام
شبیه‌ساز آموزش اپراتور	۲۰۰۲	کانادا	تائید شده	فقط خلاصه سطح بالا	ترکیبی	ناشناخته	CN	صنعت داروسازی و پزشکی	ناشناخته	هیچکدام	ناشناخته	هیچ کدام	عمدی	مخرب	بدافزار		کم	فعال	ناشناخته
تیروگاه هسته‌ای دیویس-بسه	۲۰۰۳	آمریکا	تائید شده	برخی از جزئیات	خارجی	ناشناخته	CN, SN	عمومی	ناشناخته	SD	LR	A	عمدی	مخرب	بدافزار	پیشرفته	کم	فعال	ناشناخته
اس تیلوئیس	۲۰۰۵	آمریکا	تائید شده	فقط خلاصه سطح بالا	داخلی	دیگری	FN	صنعت برق	دولتی	SD	LR, LB, PuR	A, I	تغییرعمدی	تغییر مخرب	خرابی سیستم دیگر	*	*	*	*
Tehama Colusa Authority	۲۰۰۷	آمریکا	تائید شده	فقط خلاصه سطح بالا	داخلی	کارمند سابق	SN	صنعت آب و فاضلاب	دولتی	ID, PD, AD	LB	A, I	عمدی	مخرب	استفاده نادرست از منابع	مبتدی	خیلی‌زیاد	فعال	انتقام
Ahack worm	۲۰۰۸	برزیل	تائید شده	فقط خلاصه سطح بالا	خارجی	پیمانکاران	SN, CN	فرآوری فولاد و فلزات	دولتی	SD, ID	LR, LB	A	عمدی	مخرب	استفاده نادرست از منابع	حد واسط	کم	فعال	مالی
استاکس‌نت	۲۰۱۰	ایران	تائید شده	جزئیات گسترده	ترکیبی	مهاجمان حرفه‌ای سازمان یافته	FN, LC , SN	صنعت هسته ای	دولتی	SD, DD, PD, AD	LR ,PoR	I , C , A	عمدی	مخرب	بدافزار	پیشرفته	خیلی‌زیاد	فعال	سیاسی ، تروریسم
Duqu	۲۰۱۱	برخی کشورها	تائید شده	بسیاری از جزئیات	خارجی	مهاجمان حرفه ای سازمان یافته	CN	عمومی	ترکیبی	DD	LR	C	عمدی	مخرب	بدافزار	پیشرفته	کم	تغیرفعال	ناشناخته
Shamoon	۲۰۱۲	عربستان سعودی	تائید شده	بسیاری از جزئیات	خارجی	مهاجمان حرفه ای سازمان یافته	CN	,صنعت نفت و گاز صنعت برق	تجاری - دولتی	DD,ID, SD	LR - PoR	I , C , A	عمدی	مخرب	بدافزار	پیشرفته	خیلی‌زیاد	فعال	سیاسی - مالی
Flame	۲۰۱۲	بسیاری از کشورها	تائید شده	بسیاری از جزئیات	خارجی	مهاجمان حرفه ای سازمان یافته	CN	عمومی	دولتی ،سازمان تغیرانتفاعی و فردی، آموزشی	DD	LRst	C	عمدی	مخرب	بدافزار	پیشرفته	کم	تغیرفعال	ناشناخته
Wiper	۲۰۱۲	ایران	تائید شده	بسیاری از جزئیات	خارجی	مهاجمان حرفه ای سازمان یافته	CN	,صنعت نفت و گاز صنعت برق	دولتی	ID, SD	LR, LB	A, I	عمدی	مخرب	بدافزار	پیشرفته	کم	فعال	ناشناخته
Havex	۲۰۱۴	بسیاری از کشورها	تائید شده	بسیاری از جزئیات	خارجی	مهاجمان حرفه ای سازمان یافته	SN	صنعت هسته ای , صنعت برق	دولتی	DD, SD	LR, LB	C , A	عمدی	مخرب	بدافزار	پیشرفته	کم	فعال	ناشناخته
Germany Steel Attack	۲۰۱۴	آلمان	تائید شده	برخی از جزئیات	خارجی	ناشناخته	CN, SN, LC	فرآوری فولاد و فلزات	ناشناخته	SD, AD	LB, LR	A	عمدی	مخرب	بدافزار	پیشرفته	زیاد	فعال	ناشناخته
Industroyer	۲۰۱۶	اکراین	تائید شده	برخی از جزئیات	ناشناخته	مهاجمان حرفه ای سازمان یافته	LC, SN	صنعت برق	دولتی	DD, ID	PuR, PoR	C , I , A	عمدی	مخرب	بدافزار	پیشرفته	خیلی زیاد	فعال	سیاسی
ClearEnergy	۲۰۱۷	بسیاری از کشورها	تائید شده	برخی از جزئیات	خارجی	ناشناخته	LC, SN, CN	عمومی	ناشناخته	ID, DD	LB, LR	A , C	عمدی	مخرب	بدافزار	پیشرفته	کم	فعال	مالی
Triton	۲۰۱۷	ناشناخته	تائید شده	برخی از جزئیات	ناشناخته	مهاجمان حرفه ای سازمان یافته	LC, FN	ناشناخته	ناشناخته	SD, AD	ناشناخته	A, I	عمدی	مخرب	بدافزار	پیشرفته	زیاد	فعال	سیاسی

* کد اختصاصی

۵– نتیجه گیری

بی شک ظهور سیستم‌های صنعتی از جمله DCS و اسکادا و اتصال آن به شبکه جهانی، تاثیر شگرفی در توسعه فرایندهای کنترلی زیرساخت‌های حیاتی کشورها، به ویژه نظارت و کنترل تجهیزات از راه دور داشته است. هرچند این پیشرفت و توسعه، آسیب‌پذیری‌های جدیدی را نیز به همراه داشته که بحث امنیت سایبری سیستم‌های کنترل صنعتی را به چالش کشیده است. از این منظر شناخت کامل بسترها و بخش‌های آسیب‌پذیر و همچنین تهدیدات ناشی از آنها امری لازم و ضروری است. پس از شناخت بخش‌های آسیب‌پذیری سیستم‌های صنعتی، بررسی راهکارهای تدافعی و بهبود سطح ایمنی، از جمله اقداماتی است که در کاهش تهدیدات و خطرات احتمالی نقش بسزایی دارد. ازجمله مهمترین این اقدامات می‌توان به بهره‌گیری از استانداردها و توصیه نامه‌های ارتقاء امنیت سایبری اشاره کرد.

مراجع:

[1] Geric S, Hutinski Z. Information system security threats classifications. Journal of Information and Organizational Sciences.(2007) Jun 12;31(1):51-61.
[2] ISA/IEC-62443-1-1 Industrial communication networks , Network and system security,(2009).
[3] Ruf L, AG C, Thorn A, GmbH A, Christen T, Zurich Financial Services AG, Gruber B, Credit Suisse AG., Portmann R, Luzer H, Thr eat Modeling in Security Architecture - The Nature of Threats. ISSS Working Group on Security Architectures, (2008)
[4] Alhabeeb M, Almuhaideb A, Le P, Srinivasan B. Information Security Threats Classification Pyramid. 24th IEEE International Conference on پیشرفته Information Networking and Applications Workshops: (2010). p. 208-213, doi: 10.1109/WAINA.2010.39.
[5] R. Shirey, Security Architecture for Internet Protocols: A Guide for Protocol Designs and Standards, Internet Draft: draft -irtf-psrg-secarch-sect1-00.txt (Nov. 1994).
[6] Bishop, Matt. Introduction to computer security, Boston, MA: Addison-Wesley, 2005.
[7] Swiderski F, Snyder W. Threat Modeling. Microsoft Press; 2004.
[8] ISO 7498-2,Information processing systems, Open Systems Interconnection, Basic Reference Model, 1989.
[9] Jouini, Mouna, Latifa Ben Arfa Rabai, and Anis Ben Aissa. "Classification of security threats in information systems." Procedia Computer Science 32(2014): 489-496, doi: 10.1016/j.procs.2014.05.452
[10] Howard, J. D., & Longstaff, T. A. A Common Language for Computer Security Incidents.Sandia Report # SAND98-8667.Retrieved fromhttp://prod.sandia.gov/techlib/access-control.cgi/1998/988667.pdf, (1998), October, doi: 10.2172/751004.
[11] Zhu B, Joseph A, Sastry S. A taxonomy of cyber attacks on SCADA systems. InInternet of things (iThings/CPSCom), 2011 internat ional conference on and4th international conference on cyber, physical and social computing, IEEE, (2011) Oct 19, (pp. 380-388), doi: 10.1109/iThings/CPSCom.2011.34.
[12] Miller WB, Rowe DC, Helps R, Woodside R. A Comprehensive and Open Framework for Classifying Incidents Involving Cyber-PhysicalSystems.Proceedings of The 2014 IAJC/ISAM Joint International Conference, (2014).
[13] Miller WB. Classifying and Cataloging Cyber-Security Incidents Within Cyber-Physical Systems,Brigham Young University - Provo,(2014).

[14] Kjaerland, M. A Taxonomy and Comparison of Computer Security Incidents from the Commercial and Government Sectors. Computer Security, 25(7),(2006), October, 522-538, doi: 10.1016/j.cose.2006.08.004.
[15] Blackwell, C. A Security Ontology for Incident Analysis. Proceedings of the Sixth Annual Workshop on Cyber Security and Information IntelligenceResearch, 1, (2006), October, doi: 10.1145/1852666.1852717.
[16] Hansman, S., & Hunt, R. A Taxonomy of Network and Computer Attacks. Compuer. Security, 24(1), (2005), 31-43, doi: 10.1016/j.cose.2004.06.011
[17] Simmons, C., Dasgupta, S. S., & Wu, Q. AVOIDIT: A Cyber Attack Taxonomy. University of Memphis, Technical Report # CS-09-003, (2009).
[18] Miller B, Rowe D. A survey SCADA of and critical infrastructure incidents. InProceedings of the 1st Annual conference on Research in informationtechnology, ACM, (2012) Oct 11 (pp. 51-56), doi: 10.1145/2380790.2380805.
[19] Ogie RI. Cyber Security Incidents on Critical Infrastructure and Industrial Networks. InProceedings of the 9th International Conference on Computer andAutomation Engineering, (2017) Feb 18 (pp. 254-258). doi: 10.1145/3057039.3057076.
[20] Mohammad Mehdi Ahmadian , Mehdi Shajari , Mohammad Ali Shafiee , Industrial Control System Security Taxonomic Framework with Application to a Comprehensive Incidents Survey, International Journal of Critical Infrastructure Protection (2020), doi: https://doi.org/10.1016/j.ijcip.2020.100356