OVE AKTUELL

Schwerpunkt Informationstechnik

Cyber Security

Sehr geehrte LeserInnen,

nachfolgend erhalten Sie den Newsletter **OVE Aktuell** mit dem Schwerpunkt **„Cyber Security“**.

Ein kurzer Gesamtüberblick:

1. OVE Academy Seminare/Veranstaltungen

Systematische Absicherung industrieller Automatisierungssysteme mit der IEC 62443
Gefahren für Anlagen realistisch beurteilen, objektiv analysieren und dokumentieren systematisch Maßnahmen ergreifen, um die Risiken zu senken

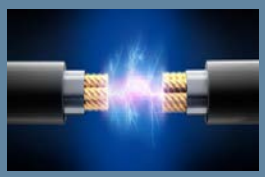
Termin
Di., 19.01.2021 – Mi. 20.01.2021

OVE E 8101 und OVE-Richtlinie R 12-2
Rechtssicherheit bei Anwendung der OVE E 8101
Rechtsstatus und Struktur der Errichtungsbestimmung OVE E 8101

Termin
Mi., 18.11.2020 von 9.00 – 16.00 Uhr

Planungsgrundsätze für die Errichtung von Trafostationen
Vorschriftenlage in Österreich, Einreichverfahren und Projektunterlagen, Störlichtbogenthematik etc.

Termin
Do., 19.11.2020 von 9.00 – 16.00 Uhr



Beherrschung von Störlichtbögen in Mittelspannungsanlagen
Normenkonforme Lösungen für Trafostationen

Termin
Mi., 25.11.2020 von 9.00 – 16.00 Uhr

2. Einleitung

Dipl.-Ing. Thomas Bleier, MSc
OVE Informationstechnik
Arbeitsgruppenleiter „Cyber Security“
OVE-OEK Vorsitzender der AG MR 65
Industrial Automation & Control System Security
Geschäftsführer B-SEC better secure KG
Kontakt: t@b-sec.net

Erkennen von Angriffen in OT-Umgebungen

Das Jahr 2020 hat uns wie wohl kein anderes in der jüngeren Geschichte Flexibilität in Bezug auf das Reagieren auf neue Situationen und Veränderungen abverlangt. Niemand würde auf die Idee kommen, trotz eines veränderten Umfeldes sein gewohntes Leben weiterzuleben und die Erkenntnisse aus den aktuellen Entwicklungen nicht in sein Verhalten einfließen zu lassen.

Im IT- und insbesondere auch im OT-Umfeld finden wir leider oft eine Situation vor, die sich durchaus so beschreiben ließe – Veränderungen in der Bedrohungslandschaft und Angriffe werden nicht rechtzeitig erkannt und berücksichtigt, die Sicherheitsmaßnahmen werden nicht angepasst, und auf Angriffe wird erst reagiert, wenn es schon zu spät ist.

Die mittel- und langfristige Anpassung an veränderte Bedrohungslagen ist ein wichtiges Element auf der strategischen Seite; in diesem Newsletter soll es aber vor allem um die kurzfristige Erkennung von und Reaktion auf Angriffe gehen. Sicherheitsmaßnahmen können noch so gut geplant und umgesetzt sein: aber kein System ist 100 % sicher, und sowohl die reale Welt als auch IT-Umgebungen zeigen uns immer wieder, dass auch Situationen, die man nicht für möglich gehalten hätte, eintreten können. Entscheidend für die erfolgreiche Bewältigung sind das rasche Erkennen der Lage und die ebenso rasche Reaktion, um Schlimmeres verhindern zu können. Im Bereich der IT spricht man hierbei von detektiven und reaktiven Sicherheitsmechanismen, und in den letzten Jahren haben Technologien wie Logdatenmanagement und -analyse oder SIEM (Security Information and Event Management) massiv an Bedeutung gewonnen, um den Bedrohungen der heutigen Zeit begegnen zu können.

Gerade im Bereich der automatisierten Erkennung von Angriffsmustern stehen wir am Anfang einer Entwicklung, bei der KI und Machine Learning-Technologien den Automatisierungsgrad in diesem Bereich massiv steigern sollen, um die ebenso massiv steigende Anzahl an Angriffen bewältigen zu können. Florian Skopik beschäftigt sich am AIT Austrian Institute of Technology seit einigen Jahren mit diesem Forschungsthema und gibt im ersten Artikel einen Überblick über die aktuell verwendeten Methoden und Lösungsansätze, die auch in seiner Forschungsgruppe in verschiedenen Einsatzszenarien evaluiert und weiterentwickelt werden.

Nachdem diese Technologien allgemein anwendbar sind und im IT-Bereich seit einigen Jahren verstärkt eingesetzt werden, finden sie in letzter Zeit auch im OT-Bereich immer häufiger Anwendung – nicht zuletzt deshalb, weil auch Best Practices und Standards wie die IEC 62443 detektive und reaktive Sicherheitsmaßnahmen einfordern. Gerhard Kratschmar von Antares NetlogiX zieht im zweiten Artikel einen interessanten Vergleich zur Luftfahrt, wo ebenso Monitoring-Mechanismen zur frühzeitigen Erkennung kritischer Situationen eingesetzt werden. Sein Unternehmen bietet eine in Österreich entwickelte Lösung für diesen Themenbereich an, die auch in einigen OT-Umgebungen bereits im Einsatz ist.

Noch ein Hinweis in eigener Sache: Die für diesen Herbst geplante Veranstaltung zur IEC 62443 wurde aufgrund der Situation rund um COVID19 auf das nächste Jahr verschoben – wir hoffen, im Herbst 2021 wieder einen Event mit spannenden Erfahrungsberichten und der Möglichkeit zum persönlichen Austausch über den aktuellen Entwicklungsstand der IEC 62443 organisieren zu können.

Wie immer möchte ich mich wieder sehr herzlich bei den Autoren für ihre Beiträge bedanken, und lade Sie dazu ein, Ihre Meinungen und Erfahrungen zu diesen oder anderen relevanten Themen im Bereich der OT Security in künftigen Newsletter-Beiträgen mit uns zu teilen.

3. Logdatenanalyse mittels Machine Learning

Dr. Dr. Florian Skopik
AIT Austrian Institute of Technology

Ein Ausblick

Zur Erkennung von Angriffen werden heute immer noch überwiegend signaturbasierte Netzwerk-IDS-Ansätze (NIDS) verwendet. In ähnlicher Weise können signaturbasierte HIDS hostbasierte Quellen verwenden, um Angriffsversuche zu identifizieren. Das Geheimnis ihrer Erfolge liegt in der einfachen Anwendbarkeit und der niedrigen Falsch-Positiv-Rate. Bedauerlicherweise hat diese einfache Anwendbarkeit aber auch ihren Preis. Die geringste Änderung an der Malware oder der Konfiguration des Angreifer-Tools ändert die Spuren, die ein Angriff auf einem System bzw. in den zahlreichen Protokolldateien hinterlässt, wodurch die Effektivität signaturbasierter Ansätze stark eingeschränkt wird.

Zum Beispiel haben Untersuchungen gezeigt, dass bekannte Malware viele HIDS umgehen kann, indem sie einen einzelnen NOP-Befehl an der richtigen Stelle ihres Codes implementiert. Automatisiert erstellte Derivate von Schadsoftware aus dem Baukasten – die Branche spricht von etwa vier neuen Malware-Samples pro Sekunde, die in den weltweiten Malware-Labs (ebenfalls überwiegend automatisiert) untersucht werden müssen, um Signaturen zu extrahieren – tun ihr Übriges.

Infolgedessen findet ein wichtiger Wandel, weg von signaturbasierten Blacklisting-Ansätzen hin zu verhaltensbasierten Whitelisting-Ansätzen, statt. Die Grundidee ist, statt bösartiges Verhalten zu modellieren und danach zu suchen, dies mit erwünschtem Verhalten zu tun (d. h. auf eine Whitelist zu setzen) und alles andere als potenziell problematisch zu klassifizieren. So funktionieren Anomalieerkennungsmethoden (AD).

AD-Ansätze sind flexibler als signaturbasierte Ansätze und können neuartige und bisher unbekannte Angriffe erkennen. Anomalieerkennungsansätze (AD) basieren auf maschinellem Lernen, um das normale (gewünschte) Verhalten eines Systems zu bestimmen. Es gibt drei Möglichkeiten, wie selbstlernende AD realisiert werden kann: „Unsupervised Learning“ erfordert keine vorklassifizierten Daten und kann lernen, während einer Trainingsphase zwischen normalem und böswilligem Systemverhalten zu unterscheiden. Basierend auf den Ergebnissen klassifiziert es alle anderen gegebenen Daten während der Erkennungsphase.
„Semi-Supervised Learning“ impliziert, dass der Trainingssatz nur anomaliefreie Daten enthält und wird daher auch als „Ein-Klassen“-Klassifikation bezeichnet.
„Supervised Learning“ erfordert einen vollständig vorklassifizierten Trainingssatz, der Daten sowohl zu normalem als auch zu unerwünschten Aktionen enthält.

Meist wird sodann zwischen sechs Klassen von AD-Algorithmen unterschieden: „Statistische AD“ ist eine semi-supervised Methode, wobei ein Modell das erwartete Verhalten des Systems definiert und Daten, die von diesem Modell abweichen, als Anomalien markiert werden. Statistische AD beinhaltet einfache Algorithmen, die bei komplexen Angriffen oft an ihre Grenzen stoßen. „Klassifizierungsbasierte AD“ verwendet eine Klassifizierungsfunktion, um diese auf zwei oder mehr Datenkategorien zu trainieren, normalerweise auf

gutartige Samples und Angriffs-Samples. Optional können Angriffe in Unterkategorien unterteilt werden, z. B. DoS-Angriffe, Intrusions und bösartige Softwareinfektionen. Im Produktionsmodus signalisiert das System Samples, die nicht gutartig kategorisiert sind. Die Klassifizierung wird überwacht, abhängig von der korrekten Kategorisierung aller Trainingsmuster.

„Clustering-basierte AD“ ist eine unsupervised Methode zur Erkennung von Anomalien. Beim Clustering werden Stichproben mit gemeinsamen oder ähnlichen Eigenschaften – den so genannten Features – unterschiedlichen Clustern zugewiesen. Beispielsweise können Flussdaten mit Merkmalen wie Flussdauer, Anzahl der Bytes, Quell- und Ziel-IP-Adresse usw. basierend auf diesen Merkmalen geclustert werden. Einige charakteristische Merkmale, beispielsweise eine bestimmte Portnummer oder ein bestimmter Adressbereich, können dann einen Angriff identifizieren. Die Hauptherausforderungen für das Clustering umfassen die Identifizierung anomaler Cluster sowie die Definition ihrer Grenzen (d. h. das Festlegen der optimalen Grenze zwischen gutem Verhalten und anomalen Verhalten).

Der Vollständigkeit halber soll auch die „Wissensbasierte AD“ genannt werden. Sie verwendet eine Liste bekannter Angriffe und vergleicht für jedes Datensample, ob es mit einem bekannten Angriffsmuster übereinstimmt. Dies kann mithilfe eines regulären Ausdrucks oder eines einfachen Byte-weisen Abgleichs aller eingehenden Pakete erfolgen.

„Ensemble-Methoden“ kombinieren mehrere Methoden für ihre Entscheidung. Beispielsweise kann man fünf verschiedene Klassifizierungsfunktionen anwenden und mithilfe einer Mehrheitsentscheidung festlegen, ob ein Sample als Anomalie betrachtet werden soll.

„Maschinelles Lernen (ML) basierend auf AD“ wird oft als eigenständige Kategorie betrachtet, verwendet aber defacto „nur“ ein Ensemble von Methoden und Technologien, die typischerweise für die Klassifizierung und Cluster-Bildung verwendet werden.

In Forschung und Industrie herrscht die allgemeine Auffassung vor, dass AD-basierte Lösungen das Problem veralteter Signaturen effektiv lösen können. AD-basierte Systeme haben jedoch ihre eigenen Tücken: Ihre Konfiguration ist meist komplex und ressourcenintensiv, die Wartung in kurzen Zyklen ist unerlässlich, und sobald sie unter hohen Falsch-Positiv-Raten leiden, verlieren die Nutzer schnell das Vertrauen in diese Technologie. Eine vielversprechende Lösung für dieses Problem besteht darin, maschinelles Lernen anzuwenden, um mit minimalem menschlichem Eingriff eine Verhaltens-Baseline für ein beobachtetes System zu erstellen und in Folge auch auf dem neuesten Stand zu halten. Eine solche Baseline kann somit beispielsweise charakterisieren, welche Features von Programmen und Diensten durch welche Benutzer verwendet, welche Prozesse in welchen Zeitintervallen gestartet werden, über welche Protokolle und Ports sie kommunizieren oder grundsätzlich, wie einzelne Maschinen in einem komplexen Netzwerk untereinander interagieren. Die dafür verwendbaren Datenquellen sind mannigfaltig und deren gezielte Auswahl meist eine große Herausforderung. Insbesondere kann maschinelles Lernen an zwei Fronten von Nutzen sein: Erstens, um zu erkennen, welche Daten und Datenmerkmale tatsächlich nützlich und relevant sind, um Anzeichen von Systemeinbruch, Missbrauch und Modifikation zu erkennen und daher überhaupt zu beobachten sinnvoll sind. Dies beinhaltet ferner die automatische Erstellung von Parsern für Daten mit unbekannten Strukturen und die Extraktion von Informationen mit hoher Entropie. Im Detail bedeutet dies, dass eruiert wird, welche Teile einer Logzeile oder eines Pakets im Netz die informationstragenden Token darstellen. So kann beispielsweise in Logdaten identifiziert werden, an welchen Stellen variable Daten, wie beispielsweise Systemnamen, IP-Adressen, Portnummern, Benutzernamen, Domänen, Dateinamen und -pfade usw., zu finden sind, wohingegen an anderen Stellen entweder statische Elemente (die festen Bestandteile einer Logzeile oder eines Netzwerkpakets) oder zufällige Daten (Session-Nummern und dergleichen) zu finden sind und im Allgemeinen weniger zur Erkennung von schadhaftem Verhalten beitragen.

Zweitens wird maschinelles Lernen angewendet, um eine Regelbasis zum Analysieren und Interpretieren beobachteter Daten zu erlernen und aufrechtzuerhalten, also zu schauen, welche Schwellenwerte unter normalen Umständen erwartet werden (z. B. Anzahl von Login-Events eines Benutzers in einem vorgegebenen Zeitfenster, Anzahl von Requests an eine Web-Applikation, aber auch komplexere Verhältnisse, wie etwa die Anzahl von HTTP POST zu GET-Requests), und um Beziehungen (Korrelationen) von Datenelementen aufzudecken. Beispielsweise können so automatisiert statistische Zusammenhänge zwischen User Agents und IP-Adressen in Web Access Logs erkannt oder aber auch SSH Fingerprints zu Maschinennamen assoziiert werden – und in weiterer Folge statistische Abweichungen dieser Korrelationen ermittelt werden. In der Forschung gibt es eine Vielzahl von Ansätzen, Konzepten und Algorithmen für maschinelles Lernen, die statistische Abweichungen ohne menschlichen Aufwand erkennen können. Die Auswahl geeigneter Ansätze hängt hauptsächlich vom Anwendungsfall und den Umständen, insbesondere Datenvielfalt, -komplexität und -qualität ab. Insbesondere für cyber-physische Systeme und IoT-Anwendungen sehen diese jedoch besonders vielversprechend aus. Prozesse in diesen Systemen sind üblicherweise streng deterministisch, es gibt keine menschlichen Nutzer, deren abweichendes Verhalten Analysen negativ beeinträchtigen, und einmal in Betrieb genommene Systeme werden nur selten verändert.

Wie können Machine Learning-Ansätze nun in der Praxis zum Einsatz gebracht werden?

Hat man sich die Grundlagen des Logdatenamanagements angeeignet, dann bietet die Open Source Lösung AECID[1] eine einfache Möglichkeit, sich mit der komplexen Materie des Machine Learnings Schritt-für Schritt vertraut zu machen:

- Lernen Sie, wie Protokolldaten auf skalierbare Weise analysiert und normalisiert werden, d. h. ohne ineffiziente lineare Listen regulärer Ausdrücke.
- Lernen Sie, wie Protokollereignisse in Echtzeit effizient geclustert werden, d. h. Cluster schrittweise erstellt werden, während Protokollereignisse eintreffen.
- Lernen Sie, wie Systeme mithilfe von Cluster-Maps charakterisiert und Verhaltensprofile erstellt werden.
- Erfahren Sie, wie Sie automatisch Korrelationsregeln aus Protokolldaten erstellen.
- Erfahren Sie, wie Sie Systemverhaltenstrends über die Zeit verfolgen.

Einen sanften Einstieg in diese Thematik bietet dafür das folgende Tutorial: https://github.com/ait-aecid/logdata-anomaly-miner/wiki/Getting-started-(tutorial), komplexere Beispiele sind hingegen hier zu finden: https://github.com/ait-aecid/logdata-anomaly-miner/wiki/AMiner-TryItOut

[1] https://github.com/ait-aecid

4. OT-Umgebungen

Dipl.-Ing. (FH) Gerhard Kratschmar
Compliance & Datenschutz
Antares NetlogiX

Detektive und reaktive Sicherheitsmaßnahmen

In der gewerblichen Luftfahrt hat das Sammeln von Betriebsdaten im Rahmen des Sicherheitsmanagements eine lange Tradition. Schon in den 1950er-Jahren gab es erste Modelle eines Flugschreibers („Black Box“), um nach einem Unfall die Ursachen feststellen zu können. Zusätzlich zu dieser passiven Sicherheitsmethode wird seit etwa 20 Jahren auch der laufende Flugbetrieb überwacht. Im Rahmen des „Flight Data Monitoring“ werden quantitative Flugdaten wie etwa die Einhaltung von Geschwindigkeit, Kurs und Höhe verfolgt. Die Daten dieses Monitorings werden laufend ausgewertet und mit Parametern wie etwa Flugphase oder Wetter korreliert. Ziel ist es, potenziell gefährliche Situationen im Vorfeld zu erkennen und künftig zu reduzieren.

Flugdatenmonitoring zählt somit zu einer (pro)aktiven Sicherheitsmaßnahme – man greift ein, bevor Schaden entsteht.

Genau wie in der Luftfahrt ist es in komplexen OT-Umgebungen vorteilhaft, Daten zu sammeln und auszuwerten, um dadurch die Sicherheit zu steigern. Genaueres findet sich dazu in der internationalen Normenreihe IEC 62443 (Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme).

Der Standard IEC 62443-1-1 enthält sieben Basisanforderungen (FR – Foundational Requirements) für Themenbereiche, die bei branchenübergreifenden Sicherheits- bzw. Abhärtungsmaßnahmen und Tests in Betracht zu ziehen sind. Dazu zählt neben Nutzungskontrolle, Systemintegrität, Vertraulichkeit auch die Anforderung FR6 – Rechtzeitige Reaktion auf Ereignisse (TRE – Timely Response to Events).

In der IEC 62443-3-3 Anhang C finden sich Systemanforderungen (SR – System Requirements), die die Basisanforderung detaillierter beschreiben:

- SR 6.1 Das Steuerungssystem soll für autorisierte Personen und/oder Werkzeuge schreibgeschützten Zugriff auf Audit-Protokolle bieten.

- SR 6.2 Das Steuerungssystem soll die Fähigkeit bieten, mit kontinuierlicher Überwachung der gesamten Sicherheit, unter Verwendung allgemein akzeptierter Praktiken und Empfehlungen der Sicherheitsbranche, Verstöße zu erkennen, um eine zeitnahe Behebung zu ermöglichen.

Dies charakterisiert ziemlich genau die Funktion einer SIEM(Security Incident and Event Management)-Lösung. Wichtig hierbei ist die Möglichkeit einer flexiblen Anpassung des Regelwerks zu Normalisierung der unterschiedlichen Hersteller-Eventlogs, damit ein sinnvoller Vergleich (Korrelation) der Alarme untereinander möglich ist.

Hinzu kommen folgende Eigenschaften, die bei der effizienten Überwachung einer ICS(Industrial Control System)-Umgebung hilfreich sind:

- Mehr-Augen-Prinzip bei der Eventanalyse
- Datenschutz (DSGVO-Konformität) durch Anonymisieren oder Pseudonymisieren der Daten
- Kompletter Audit Trail im System, um jegliche Regeländerungen nachvollziehen zu können

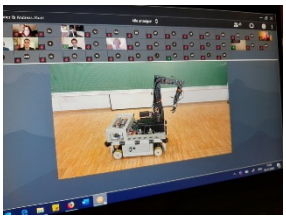
- Umfangreiche Suchfunktionen
- Einfache Bedienbarkeit bei Administration und Analyse
- Preis- und Lizenz-Gestaltung unabhängig von der Anzahl der Events und auch für KMUs geeignet

Mit diesen Anforderungen können Sie aus den Logdaten Ihrer OT-Umgebung ein wertvolles Instrument für proaktive Sicherheit gestalten.

Die LogApp des österreichischen Herstellers iQSol bietet Produktionsfirmen jeglicher Größe ein umfangreiches Feature-Set und ist auch in Smart Meter-Umgebungen und bei Energieversorgern bereits erfolgreich implementiert worden. Optional besteht auch die Möglichkeit, die gesamte Lösung als Managed ICS Security Monitoring als 8x5- wie auch als 24x7-Service zu beziehen.

Gerhard Kratschmar ist bei Antares NetlogiX als Compliance-Berater für Informationssicherheit und Datenschutz im Einsatz. Bis 2017 war er Flugkapitän und Safety-Manager bei einem Wiener Executive-Flugunternehmen. In Vorträgen, Artikeln und Podcasts zeigt er, wie sich Erkenntnisse aus dem Flugsicherheitsmanagement auf die IT/OT-Branche übertragen lassen.

6. OVE News



OVE-Energietechnik-Preis: Drei innovative Arbeiten ausgezeichnet

Ein gestengesteuertes Robotersystem, eine dynamische Simulation für die Integration von erneuerbaren Energiequellen sowie eine Decision Modell für Unternehmen, die in die Blockchain-Technologie investieren möchten: Drei innovative Abschlussarbeiten wurden mit dem OVE-Energietechnik-Preis ausgezeichnet.

Mehr…

Erneuerbaren Ausbau Gesetz: Chance für regionale Wertschöpfung

Der OVE Österreichischer Verband für Elektrotechnik begrüßt das Erneuerbaren Ausbau Gesetz, das sich derzeit in Begutachtung befindet. Das Gesetz ist eine große Chance für die regionale Wertschöpfung, Nachbesserungen braucht es noch beim Thema Energiegemeinschaften.

Mehr…

Krisensichere Jobs in der Technik: Girls! TECH UP auch Online

Die Corona-Krise beweist nicht nur, wie wichtig innovative Technik ist, sondern auch, in welchen Branchen es krisensichere Jobs gibt. Welche Möglichkeiten die Berufswelt der Technik Mädchen und jungen Frauen bietet, zeigt Girls! TECH UP künftig auch Online.

Mehr…

Wir bedanken uns für Ihre Aufmerksamkeit!

Bei Fragen, Wünschen oder Anmerkungen wenden Sie sich an informationstechnik@ove.at.

Aktuelle News aus der Welt der Elektrotechnischen Normung finden Sie bei **OVE Standardization**.

Normen, Richtlinien und Fachpublikationen können Sie in unserem **OVE-Shop** erwerben.

Wenn Sie Ihre elektrotechnischen Produkte zertifizieren lassen möchten, finden Sie hier den Kontakt zu **OVE Certification**.

OVE Österreichischer Verband für Elektrotechnik
OVE Informationstechnik, OVE Aktuell
Krenngasse 37 | 8010 Graz
T +43 316 873-7916
informationstechnik@ove.at | www.ove.at
ZVR 327279890