Angriffserkennung wirksam und effizient umsetzen

Angriffserkennung in kritischen Infrastrukturen ist seit dem IT-Sicherheitsgesetz (IT-SiG) 2.0 [1] ein vieldiskutiertes Thema. Es gibt erhebliche Unterschiede bei den Vorstellungen welche Werkzeuge und Betriebsleistungen erforderlich sind. Gerade für mittelständische Betreiber ist der Einsatz von Dienstleistungen sinnvoll. Der folgende Artikel soll Aufschluss geben welche Werkzeuge für eine wirksame Angriffserkennung erforderlich sind, warum oftmals eine Dienstleistung hier der sinnvollere Weg ist und wie die Angebote unterschieden werden können.

Ein Angriffserkennungssystem, wie es vom BSIG (§2 Abs. 9b, §8a Abs 1) [2] und EnWG (§11 Abs. 1d) [3] von Betreibern kritischer Infrastrukturen und Stromverteilungsnetze bis Mai 2023 (BSIG §8a Abs. 1a, EnWG §11 Abs. 1e) [2, 3] verlangt wird, ist ein System aus Werkzeugen, Prozessen und Spezialisten. Angriffe sollen nicht nur erkannt, sondern eben auch behandelt werden. Nur so entsteht ein konkreter Sicherheitsmehrwert.
Eines der Missverständnisse ist, dass mit der Beschaffung und Installation einer Intrusion Detection Software (IDS) diese Anforderung bereits erfüllt sei.

Die Werkzeuge zur Angriffserkennung

Im ersten Schritt wird eine Softwarekomponente benötigt, die Datenverkehr durchsucht und bei bestimmten Vorkommnissen einen Alarm ausgibt. Hier gibt es verschiedene Verfahren. Es kann einerseits nach Spuren bereits bekannter Angriffe gesucht werden (signaturbasierte Verfahren) oder nach Abweichungen von einem Normalzustand (Anomalien erkennende Verfahren). Beide Verfahren haben unterschiedliche Eigenschaften. Je nach Einsatzzweck können diese von Vor- und Nachteil sein. Beispielsweise erzeugen rein auf Anomalieerkennung basierende Werkzeuge in Netzwerken mit IT- und OT-Protokollen, wie wir sie heute bei nahezu jedem Kunden antreffen, auch ohne jeden Angriff kontinuierlich eine Unmenge von Meldungen, die dann aufwendig weiter qualifiziert werden müssen. Deshalb sollten der Systemzweck und die zu überwachende Umgebung die Tool-Auswahl bestimmen und nicht andersherum.
Wenn Sie ein Angriffserkennungssystem in Ihrer Prozessleittechnik einsetzen wollen, dann sollte dieses auch in der Lage sein neben bekannten Angriffsverfahren aus der IT auch welche auf Leittechniksysteme und Leittechnikprotokolle (wie z. B. IEC 104) zu erkennen. Viele IT IDS-Systeme können letzteres nicht. Auch im Umfang der Regelwerke und der Anpassung an die zu überwachende Anlage unterscheiden sich viele Systeme. Ein System, das weniger Alarmmeldungen verursacht, sorgt bei Kunden, die das System „nebenher" selbst betreiben wollen, erst mal für eine größere Zufriedenheit und verkauft sich damit besser. Ein trügerischer Vorteil.

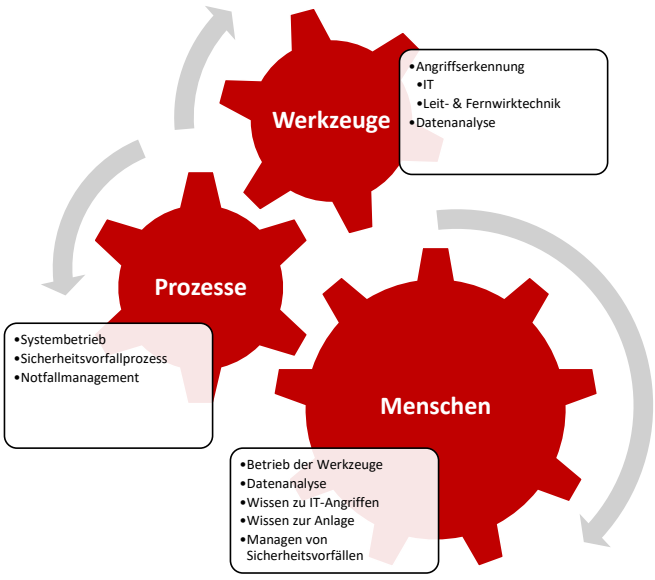

Bild 1: Bestandteile eines Angriffserkennungssystems

Rückwirkungsfrei oder besser doch nicht?

Als rückwirkungsfrei werden Werkzeuge bezeichnet, die eine Kopie des Datenverkehrs analysieren. Dabei wird die Kopie so erzeugt, dass kein Datenrückverkehr möglich ist. Hierfür gibt es unterschiedliche Verfahren. Zumeist verwendet man hierfür Mirror („Spiegel") Ports an Switches. Rückwirkungsfreiheit hat den Vorteil, dass selbst bei einer Kompromittierung des Angriffserkennungswerkzeugs kein Zugriff auf das überwachte System möglich ist. Das ist im Hinblick auf die bekannten Angriffe der letzten Vergangenheit, bei denen die Softwarehersteller für den Angriff missbraucht wurden (z. B. Solarwinds), eine sehr wirksame Sicherheitsmaßnahme.
Derselbe Vorteil gilt auch, wenn bei der Angriffserkennung ein Dienstleister beteiligt ist. Durch die Rückwirkungsfreiheit ist selbst eine Kompromittierung des Dienstleisters kein Beinbruch. Das bedeutet für das Werkzeug aber auch, dass Softwareagenten auf den Endgeräten nicht möglich sind. Ebenso wenig wie automatisierte Verbindungsabbrüche bei erkannten Verhaltensbesonderheiten, wie z. B. bei einem Intrusion Prevention System (IPS). In der Prozessleittechnik ist das aber auch weder ratsam noch erwünscht.

Proprietäre Software oder Open Source?

Im Bereich der Betriebssysteme hat das Open Source-System Linux nahezu alle anderen Systeme bis auf den Platzhirschen Microsoft verdrängt. Auch im Bereich der IT-Sicherheitswerkzeuge sind die Open Source Software (OSS)-Projekte im Vormarsch. Durch die großen und internationalen Communities sind sie nicht nur lizenzkostenfrei, sondern auch sehr innovativ und sicher. Das ist so, da der Programmcode („Source") bekannt („Open") ist. Allerdings ist für ihren Betrieb und die Nutzung ihrer

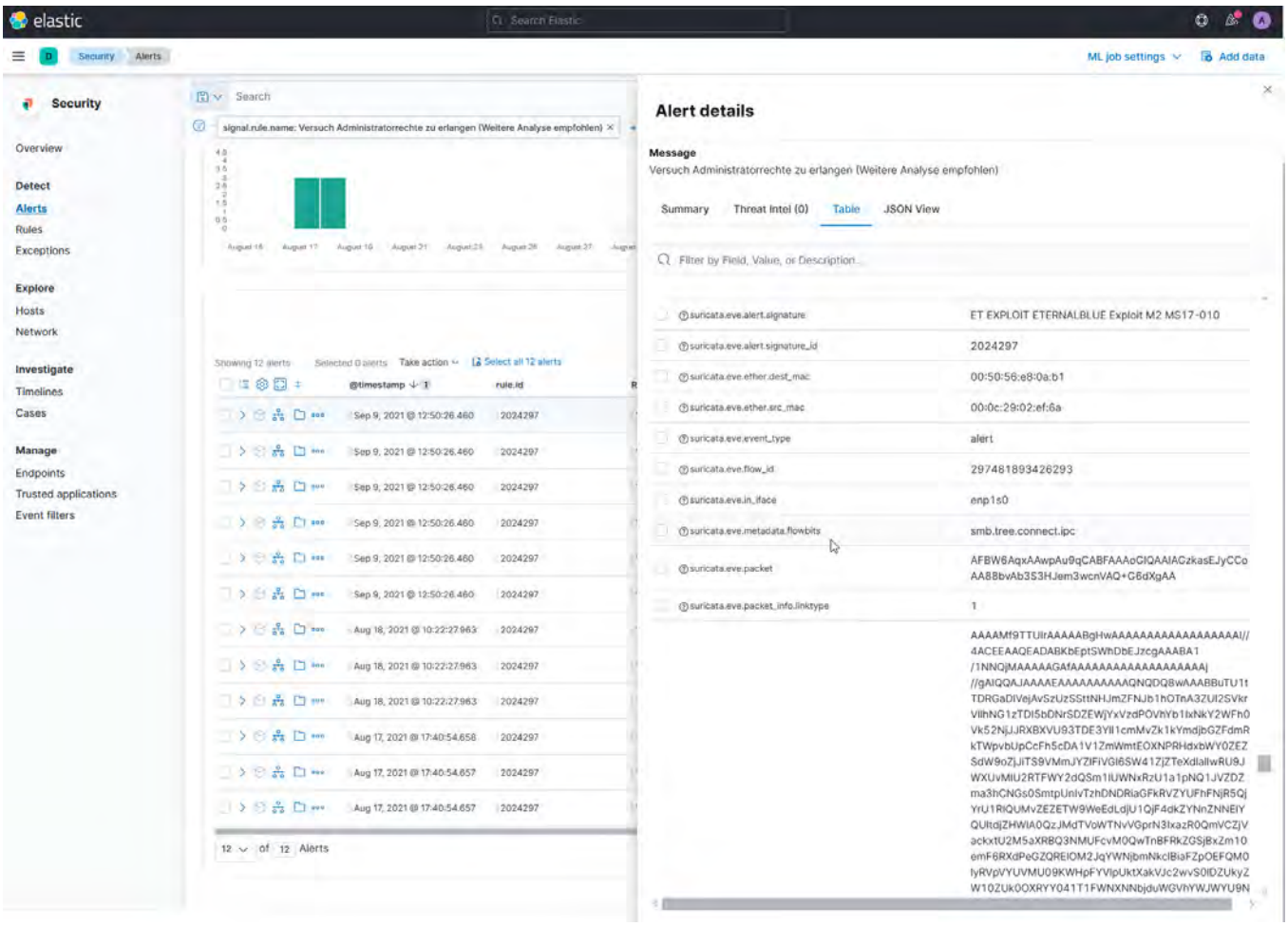

Bild 2: Alarm einer Angriffserkennungssoftware mit vielen Zusatzinformationen

oftmals sehr großen Leistungsumfänge ein profundes Wissen und das Mitarbeiten in den Projektgemeinschaften erforderlich, da es keine üblichen Hersteller mit Hotlines gibt. Viele Unternehmen, vor allem mittelständische, erschließen sich diese Vorteile durch die Nutzung spezialisierter Dienstleister.

Die Empfindlichkeit der Alarmierung – eine hohe Kunst!

Bei der Alarmierung steht die Eindeutigkeit mit der Sicherheit im Wettbewerb. Beispielsweise ist die Übertragung von ausführbaren Dateien ein sehr gutes Anzeichen für einen Angriff. Dies kommt aber bei jeder Datensicherung ebenso vor. Sollte man dieses Verhalten also alarmieren oder nicht?

Wo immer eine Kommunikation als regelmäßig nicht sicherheitsrelevant identifiziert wird, sollte sie aus der Alarmierung ausgenommen werden. Aber eben nur da. Ansonsten haben Sie mit wenigen Handgriffen das Angriffserkennungssystem unwirksam gemacht. Dieses kontinuierliche „Tuning" ist ein wichtiger Bestandteil der Betriebsarbeit.

Nachdem eine Verhaltensauffälligkeit in Ihrem Datenverkehr erkannt ist, gilt es den Kontext zu ermitteln (War es jetzt ein Angriff oder eine Datensicherung?). Dazu braucht es eine hochflexible automatisierbare „Suchmaschine" mit der effizient analysiert werden kann, was wann von wo nach wo kommuniziert wurde und ob es Ähnliches auch an anderer Stelle oder zu einer anderen Zeit gegeben hat. Hier liefern Big Data-Analysesysteme einen sehr guten Dienst. Diese sind Expertenwerkzeuge mit einer kryptisch anmutenden Bedienoberfläche. In den Händen erfahrener Spezialisten können damit aber innerhalb kürzester Zeit die erforderlichen Zusammenhänge hergestellt werden. Dabei ist die Kompetenz der Analysten allerdings weit wichtiger als das Analysewerkzeug, da oftmals ohne die richtige Frage auch keine eine klärende Antwort zu erwarten ist.

Für effizientes Tuning und Analyse ist neben sehr guten Kenntnissen der Werkzeuge ein fundiertes und aktuelles Wissen zu IT-Angriffen ebenso wie zur Netzwerktechnologie erforderlich. Auch erfolgreiche Angreifer sind innovativ und nutzen gerne, was an anderer Stelle auf dieser Welt gerade erfolgreich war.

Oft müssen Analysten kryptisch anmutende Kommunikationsdatenmitschnitte mithilfe von Suchwerkzeugen interpretieren. Hier sind IT-Spezialisten gefragt, die wissen, welches Bit & Byte an welcher Stelle welche Wirkung hat. Das gilt für IT und Leittechnik gleichermaßen, da in heutigen Leittechnikumgebungen beides gemeinsam im Einsatz ist. Ohne dieses Wissen dauert die Suche nach der Nadel im Heuhaufen sehr lange und ist zumeist hoffnungslos.

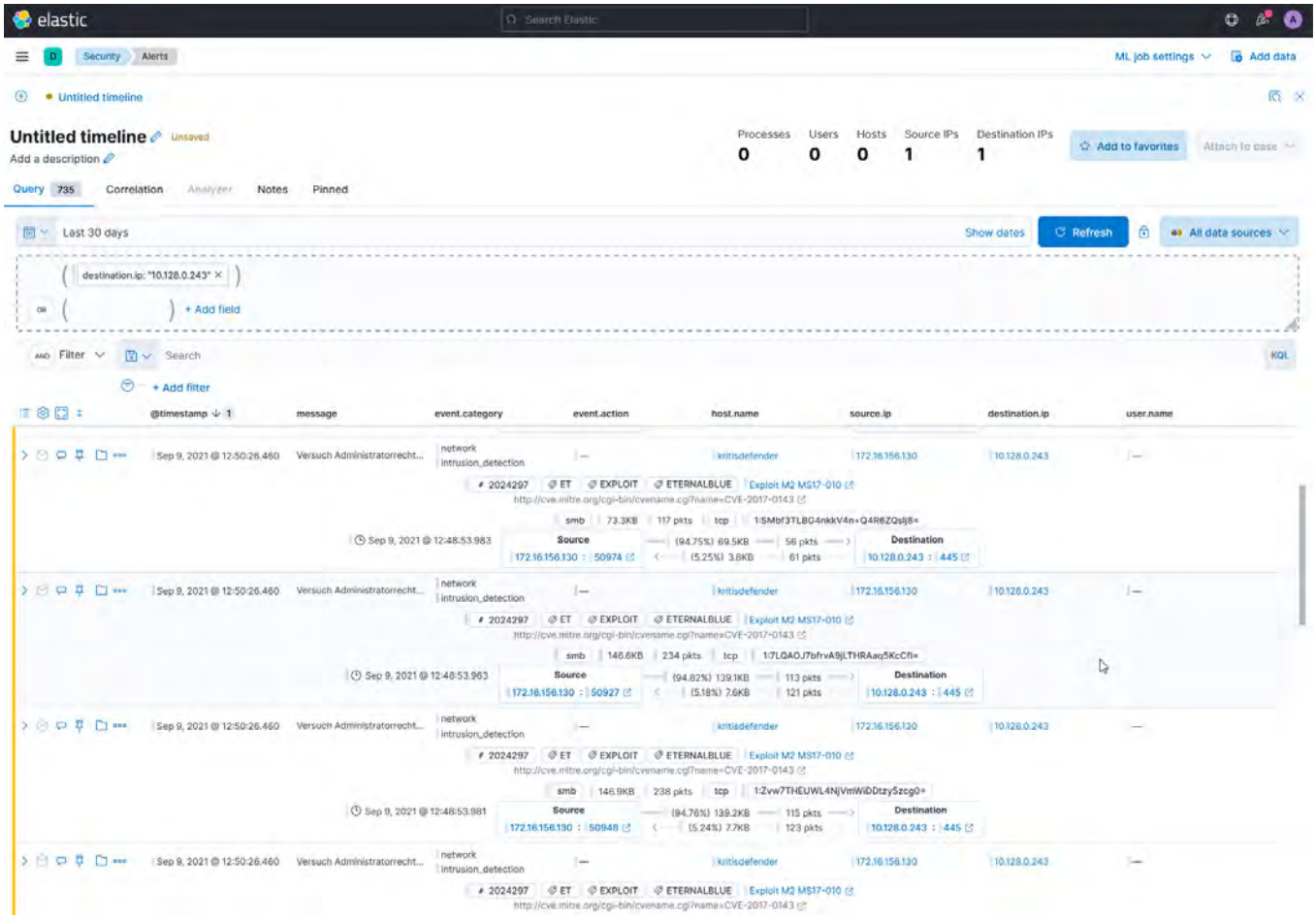

Bild 3: Kontextanalyse (timeline) eines Alarms mit Abfragewerkzeugen

Was ist, wenn ein Angriff identifiziert wurde?

Jetzt ist ein schnelles aber vor allem überlegtes Handeln erforderlich, um den entstehenden Schaden möglichst weit einzugrenzen. Dabei macht sich die Vorbereitung auf diesen Fall intensiv bemerkbar:

- wirksamer Sicherheitsvorfallprozess,
- wirksames Notfallmanagement (z. B. nach BSI 200-4),
- vereinbarte Partnerschaften (z. B. Rahmenvertrag und Arbeitsteilung mit Incident Response-Dienstleistern),
- regelmäßig geübtes gemeinsames Vorgehen aller Beteiligten.

An genau dieser Stelle kommen häufig die folgenden Fragen:

Warum kann das die Technik nicht von allein?

Viele IT-Sicherheits-Softwares bieten eine automatisierte Reaktion auf bestimmte Vorkommnisse an. Eine Grundfunktion von Firewall-Systemen ist es z. B. verbotene Kommunikation zu blockieren und zu alarmieren. Dies sollte an allen Stellen genutzt werden, wo eindeutig zwischen legitimem und illegitimem Datenverkehr unterschieden werden kann.

In den durch solche Technologien von vielen Bedrohungen geschützten Sicherheitsbereichen, wie z. B. Ihrer Leit- und Fernwirktechnik, sollte eine wirksame Angriffserkennung dann deutlich sensibler erfolgen. Hier erfordert eine eindeutige Erkennung oft weitergehende Untersuchungen. Auch die Entscheidung der weiteren Schritte (z. B. Umschalten einer Anlage auf manuellen Betrieb) mit all ihren Konsequenzen leisten Ihre erfahrenen Mitarbeiter erheblich besser als IT-Systeme.

Wir sind Mittelständler – Wir haben für Angriffserkennung weder die Mitarbeiter noch das Fachwissen!

Da die Wirksamkeit und Effizienz eines solchen Angriffserkennungssystems mit der Verfügbarkeit und Kompetenz des Betriebsteams direkt in Zusammenhang steht und ohne diese sehr schnell wirkungslos wird, liegt hier der entscheidende Faktor. Auch ist das Unterhalten eines Teams solcher Spezialisten für viele Unternehmen nicht wirtschaftlich, da Sie ja nicht andauernd angegriffen werden. Deshalb ist in sehr vielen Fällen die Zusammenarbeit mit einem geeigneten Dienstleister einfacher und vor allem deutlich wirtschaftlicher als der Eigenbetrieb. Ein weiterer Vorteil ist, dass spezialisierte Dienstleister in der Regel einfacher geeignetes Personal finden und ausbilden können.

Wenn der Dienstleister das übernimmt, was haben wir dann noch zu tun?

Die Annahme, dass der Dienstleister die Angriffserkennung komplett übernimmt, ist insbesondere in komplexen Leittechnikum-

gebungen unrealistisch. Erforderliches Detailwissen über Ihre Anlage (z. B.: Welches System verbirgt sich hinter welcher Adresse) und aktuellen Besonderheiten (z. B.: Welcher Techniker arbeitet gerade an welchem System) kann der beste Dienstleister nicht wissen. Aus diesem Grund ist es absolut sinnvoll, dass Sie in die Analyse einbezogen werden, um dann zu entscheiden, ob es sich um einen Angriff oder z. B. um eine ungeplante Entstörung handelt.

Aber verlieren wir nicht wichtiges Know-how, wenn ein Dienstleister Angriffserkennung für uns leistet?
Die regelmäßige Zusammenarbeit mit den Analysten des Dienstleisters hat tatsächlich die gegenteilige Wirkung – Ihre Mitarbeiter gewinnen kontinuierlich an Know-how. Das Wissen zu Ihrer Anlage und möglichen IT-Bedrohungen wird laufend größer. Im Vergleich zum Eigenbetrieb müssen Sie sich das Know-how aber nicht autodidaktisch in der Theorie anlernen, sondern werden in konkrete praktische Beispiele einbezogen. Erfahrene Analysten eines guten Partners erklären ihre Beobachtungen und Handlungsvorschläge verständlich und beraten Ihre Mitarbeiter auf Augenhöhe.

Unterschiedliche Dienstleistungsmodelle – unterschiedliche Dienstleistung! Was passt für wen?
Aus diesem Grund ist es wichtig, dass Sie bei der Wahl des Dienstleisters darauf achten, dass die Leistung zu Ihren Anforderungen passt:

- Sind die eingesetzten Werkzeuge auf den Einsatz in Ihrer Anlage zugeschnitten?
- Was passiert mit Ihren Daten?
- Wenn Ihre Daten beim Dienstleister verarbeitet werden (z. B. auch in dessen Ticketsystem), stellt dieser ein zusätzliches Sicherheitsrisiko für Sie dar.
- Wie gut werden die Werkzeuge kontinuierlich auf Ihre Anforderungen angepasst?
- Eine organisatorische Trennung zwischen Entwicklungs- und Betriebsteams hat hier Nachteile.
- Wie gut arbeiten die Analysten Ihres Dienstleisters mit einem diensthabenden Mitarbeiter bei Ihnen auf „Augenhöhe" zusammen (Sprache, fachliche Qualifikation, Verständnis der Anlage)?

Near- und Offshoring: Kostenoptimierung der großen Dienstleister

Große IT-Dienstleister benötigen zur Selbstverwaltung komplexe Prozesse und haben hohe Verwaltungskosten. Um dennoch wettbewerbsfähig anbieten und trotzdem Geld verdienen zu können, werden personalintensive Tätigkeiten in Billiglohnländer verlagert. Daraus ergeben sich große Herausforderungen bei der Leistungsqualität durch Unterschiede in der Zeitzone, Sprache und Kultur. Auch sorgt in diesen Ländern ein hohes Angebot an vergleichbaren Arbeitsplätzen in den Servicecentern der unterschiedlichen Anbieter für eine große Personalfluktuation. Diese hat wiederrum

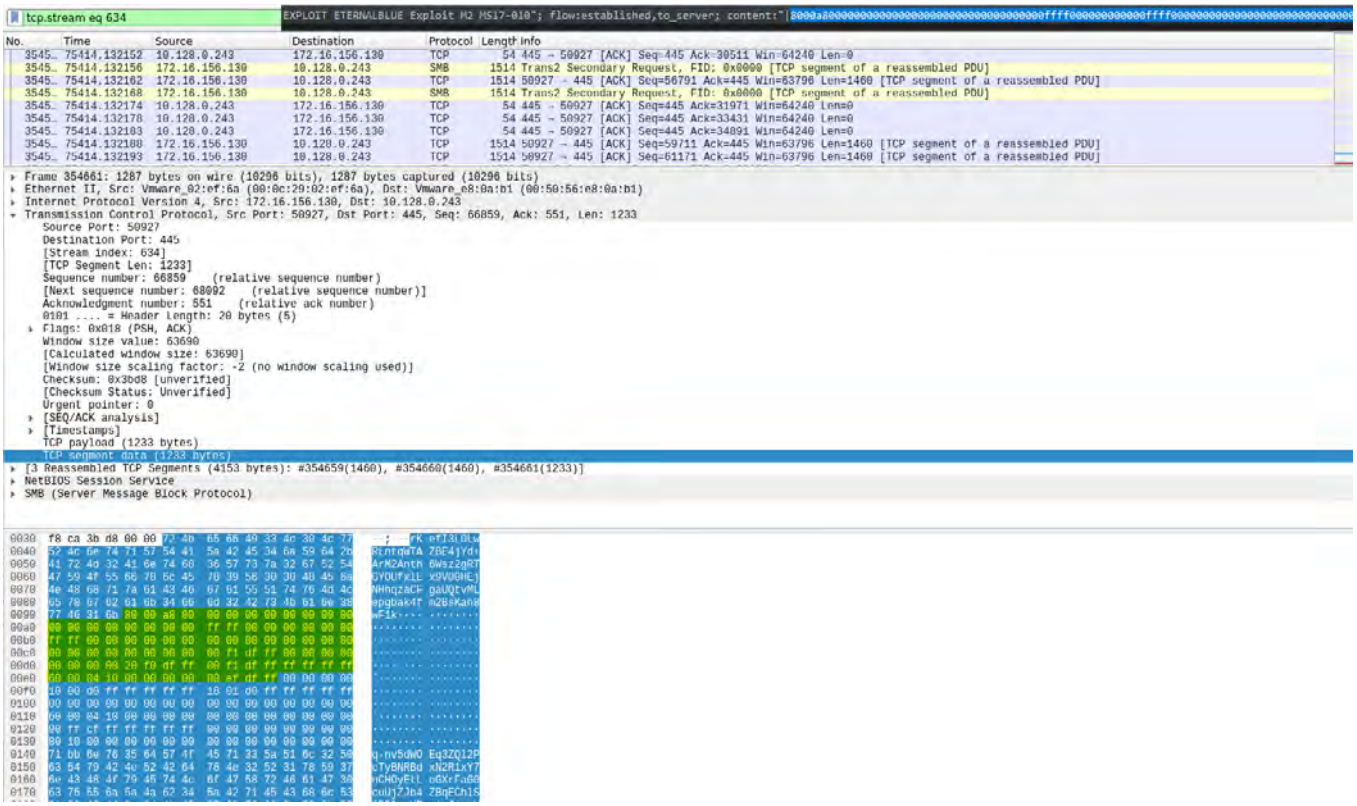

Bild 4: Auswertung von Rohdaten des Netzwerkverkehrs zur Erkennung eines Angriffs

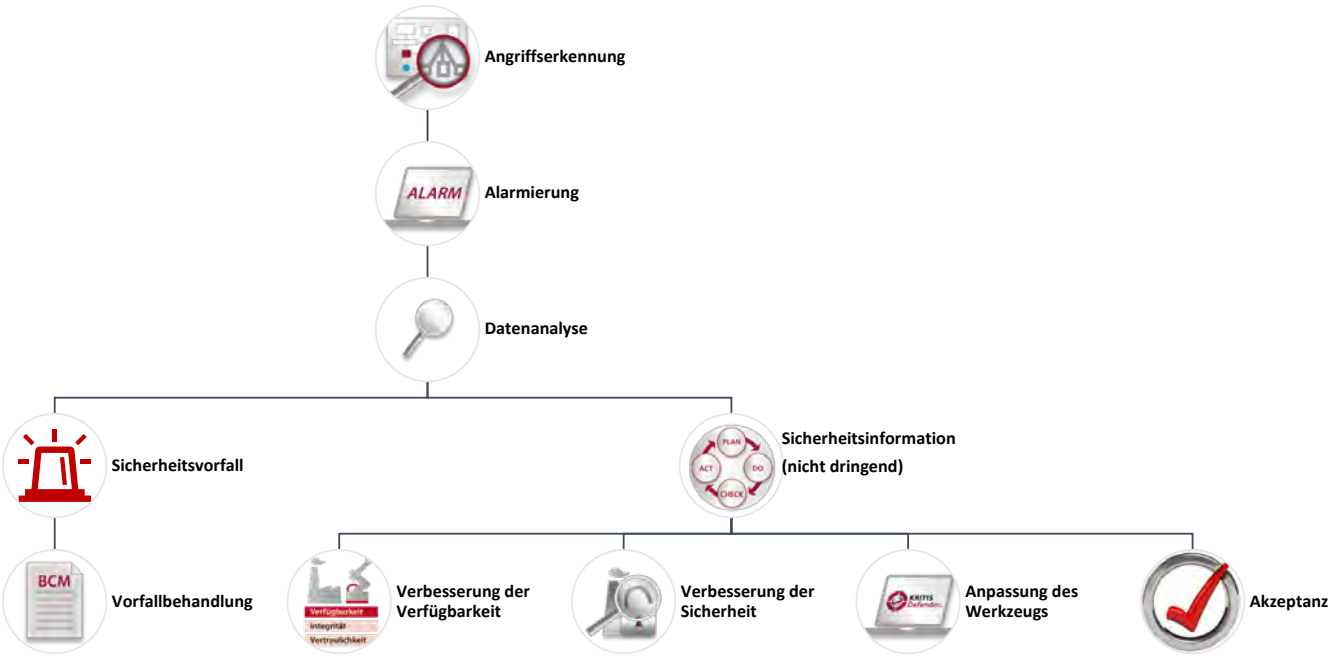

Bild 5: Prozessbild Angriffserkennung

Auswirkungen auf die Leistungsqualität (jedes Mal ein neuer Ansprechpartner, der Sie und Ihre Umgebung nicht kennt). Gerade bei IT-Sicherheitsleistungen, bei denen eine gute Kenntnis der überwachten Anlage entscheidend ist, spielt das eine große Rolle.

Angriffserkennung kann auch ohne Angriffe positive Nebenwirkungen haben

Die heute üblichen Sicherheitsmechanismen (z. B. Firewalls) wehren im Regelfall die meisten Angriffsversuche ab. Deshalb sind Angriffe in Leittechnikumgebungen eher selten. Wirksam betriebene Angriffserkennungssysteme können aber viel mehr als nur Angriffe erkennen. Einerseits werden Schwachstellen sichtbar, wie beispielsweise unverschlüsselte Passwortübertragungen. Das ist zwar banal, kommt aber regelmäßig vor und ist für einen Angreifer eine willkommene Einladung. Andererseits zeigt die Analyse des Netzwerkverkehrs auch überlastete Server und technische Defekte auf und sorgt damit für die Möglichkeit größere Probleme zu beheben, bevor sie für Störungen sorgen. Insofern liefert ein Angriffserkennungssystem einen dauerhaften Mehrwert für Sicherheit und Verfügbarkeit. Allerdings nur, wenn es von Personen betrieben wird, die derartige Zusammenhänge aus den Daten analysieren und interpretieren können und wenn die gefundenen Schwachstellen in den regelmäßigen Verbesserungsprozess aufgenommen werden (KVP).

Fazit

Angriffserkennung in der Leit- und Fernwirktechnik ist kein Mitnahmeprodukt, sondern eine Spezialdisziplin von Sicherheitsexperten. Zwischen einer IDS-Software, die gelegentliche Alarme erzeugt, und einem wirksam betriebenen Angriffserkennungssystem besteht ein himmelhoher Unterschied, welchen hoffentlich ein Auditor eher bemerkt als ein Angreifer.

Aus meiner Erfahrung ist ein wirtschaftlicher Eigenbetrieb nur den Betreibern großer Umgebungen im Rahmen eines eigenen Security Operation Centers (SOC) vorbehalten. Für alle anderen ist ein geeigneter Dienstleister die richtige Wahl. Aber auch hier ist der Vergleich wichtig, um den passenden Partner zu finden. Das ist auch die Erkenntnis der Mehrheit der Anlagenverantwortlichen und Sicherheitsbeauftragten (ISB), mit denen ich in den letzten Monaten gesprochen habe.

Da sich funktionierende Sicherheit nur in der Praxis zeigt, ist insbesondere die Übung von Sicherheitsvorfällen eine rare, aber wichtige Aufgabe und nur in zweiter Linie ein sehr geeigneter Nachweis für den Auditor.

Literatur:

[1] IT-SiG 2.0, Bundesgesetzblatt Jahrgang 2021 Teil 1 Nr. 25

[2] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik BSI-Gesetz §8a 1a), BSI-Gesetz §2 9b) https://www.gesetze-im-internet.de/bsig_2009/

[3] Energiewirtschaftsgesetz – EnWG §11 1d) https://www.gesetze-im-internet.de/enwg_2005/index.html

Autor

Sascha Jäger
Geschäftsführer
ausecus GmbH
www.ausecus.com
info@ausecus.com