vgbe energy journal

International Journal for Generation
and Storage of Electricity and Heat

9 · 2022

Angriffserkennung in Leit- und Fernwirktechnik als Dienstleistung

Sascha Jäger

Sonderdruck

ISSN 1435–3199 · K 43600 | International Edition | Publication of vgbe energy e.V.

be informed www.vgbe.energy

Über den Autor

Sascha Jäger ist Geschäftsführer und Gesellschafter bei der ausecus GmbH.
Von 1996 bis 2013 war er in unterschiedlichen Positionen bei dem IT-Security Spezialisten Integralis/NTT in Deutschland, Österreich, Schweiz und Frankreich tätig, zuletzt als Geschäftsführer. Anschließend war er bei Fujitsu für den Aufbau des Bereichs Cybersecurity (Security Operations Center) in Zentraleuropa verantwortlich und leitete diesen bis zu seinem Start bei ausecus im Januar 2021.

ausecus bietet mit seinem Service KRITIS Defender ein Angriffserkennungssystem als Dienstleistung an, das speziell für mittelständische Betreiber Kritischer Infrastrukturen entwickelt wurde. Zu den Kunden von ausecus zählen vor allem EVUs, Kraftwerksbetreiber und Stadtwerke aber auch mittelständische Unternehmen im deutschsprachigen Raum.

Sascha Jäger
ausecus GmbH
Geschäftsführer
Augsburg

i www.ausecus.com
e info@ausecus.com
t 0821 207097 - 0

Angriffserkennung in Leit- und Fernwirktechnik als Dienstleistung

Sascha Jäger

Abstract

Intrusion detection for ICS as a service

Intrusion detection for industrial control systems (ICS) is currently a hot topic due to the obligations of the German 2nd IT-Security Law (IT-SiG 2.0).

This article shows the technical requirements and legal specifications for a cyberattack detection system for KRITIS operators. These can only be performed effectively and efficiently in-house by larger organizations. For everyone else, the use of service providers is worthwhile. The author shows the important attributes when selecting the right partners and in addition, different applications for specific needs are explained.

The German security company ausecus had developed an intrusion detection system some time ago. It is based on their knowledge of cyber-attacks and vulnerabilities in ICS infrastructures of critical infrastructure operators. The system delivered very good results. Nevertheless, the customer feedback was not as good as anticipated. The customer's existing specialist staff was tied up in other tasks and therefore, a permanent in-house operation was not affordable. In addition, the alarms of such systems cannot be planned.

As a result of this experience and the requirements of the pilot customers, a cyberattack detection service for IT and ICS of utility provider was established.

Angriffserkennung in der Leit- und Fernwirktechnik von Energie- und Wasserversorgern ist seit dem IT-SiG 2.0 [1] ein vieldiskutiertes Thema. Es gibt erhebliche Unterschiede bei den Vorstellungen, welche Werkzeuge, Prozesse und Betriebsleistungen erforderlich sind. Gerade für mittelständische Betreiber ist der Einsatz von Dienstleistungen sinnvoller als der Versuch es mit Bordmitteln zu schaffen. Der folgende Artikel soll hierüber und über die gesetzlichen Anforderungen mehr Aufschluss geben. Deshalb orientiert er sich in der Struktur und den verwendeten Begriffen an der Orientierungshilfe des Bundesamt für Sicherheit in der Informationstechnik – BSI für Systeme zur Angriffserkennung, im Folgenden OH beziehungsweise SzA genannt. Außerdem soll er dabei helfen, die verschiedenen Dienstleistungsangebote zu unterscheiden.

1.1 Ein System zur Angriffserkennung ist…

Ein System zur Angriffserkennung, wie es vom Gesetz über das Bundesamt für Sicher-

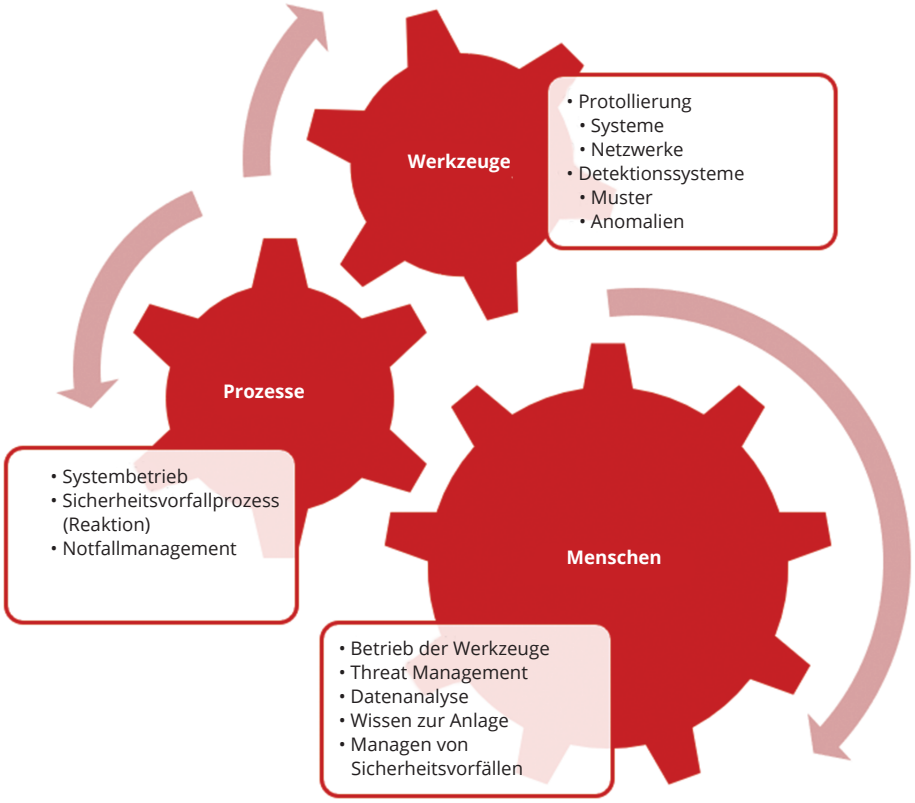

Bild 1. Bestandteile eines Angriffserkennungssystems.

Autor

Sascha Jäger
Geschäftsführer
ausecus GmbH
Augsburg, Deutschland

heit in der Informationstechnik – BSIG (§2 Abs. 9b, §8a Abs 1) [2] und Energiewirtschaftsgesetz (Gesetz über die Elektrizitäts- und Gasversorgung) EnWG (§11 Abs. 1d) [3] von Betreibern Kritischer Infrastrukturen und Stromverteilungsnetzen bis Mai 2023 (BSIG §8a Abs. 1a, EnWG §11 Abs 1e) [siehe 2; siehe 3] verlangt wird, ist ein System aus Werkzeugen, Prozessen und Spezialisten. Angriffe sollen nicht nur erkannt, sondern auch behandelt werden. Nur so entsteht ein konkreter Sicherheitsmehrwert (Bild 1).

Eines der großen Missverständnisse dabei ist, dass mit der Beschaffung und Installation einer Software für Intrusion Detection (IDS) und oder Logmanagement bzw. Security Information & Event Management (SIEM) diese Anforderung erfüllt werden könnte. Damit es dazu nicht kommt, konkretisiert das BSI mit der OH die Auslegung.

1.2 Die Orientierungshilfe des BSI – mehr als nur eine Orientierungshilfe?

Die OH als Interpretationshilfe der Gesetzesvorgaben wurden bereits mit deren Veröffentlichung zum 01.04.2021 angekündigt. Am 29.09.2022 hat das BSI die Orientierungshilfe veröffentlicht (Bild 2).

In der OH beschreibt das BSI die Bestandteile eines SzA und klassifiziert die Elemente und Ausbaustufen in MUSS, SOLL und KANN. Anhand der Prüfung und, wenn möglich, Anwendung dieser Komponenten wird auch der Reifegrad gemessen. Die OH ist damit weniger eine Empfehlung als vielmehr eine konkrete Ordnung. Sie gibt einen klaren Prüfungsprozess und eindeutige Prüfungsziele vor, die für eine Gesetzeserfüllung umgesetzt werden müssen. Dieser Charakter wird dadurch unterstrichen, dass die für den Nachweis erforderlichen Vorlagen im Anhang der OH zu finden sind.

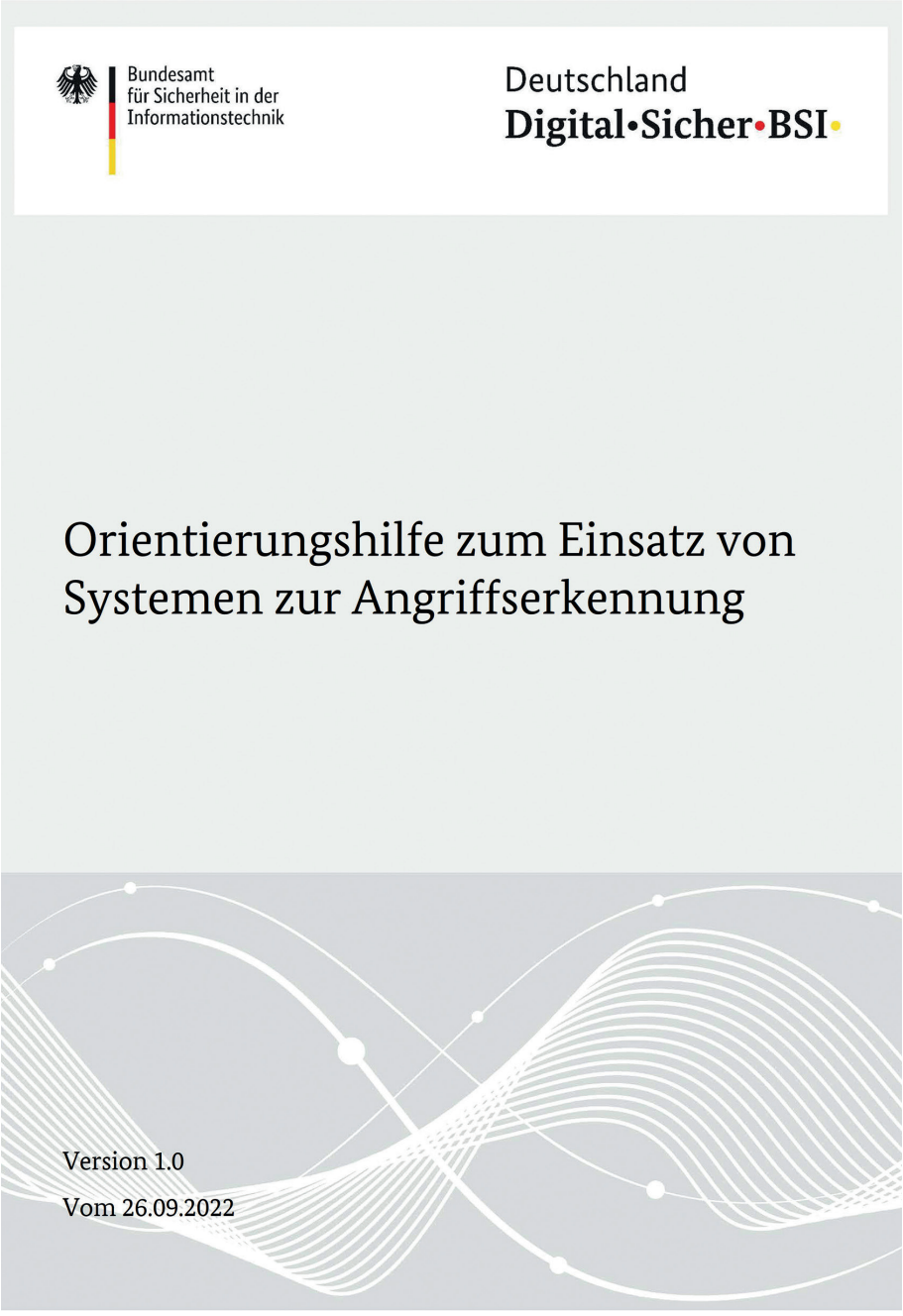

Bild 2. Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung enthält auch die Vorgaben für den Nachweis.

Auf folgende Punkte wird in der OH besonderes Augenmerk gelegt:

- Vollumfängliche Planung. Das bedeutet, auch wenn Systeme/Daten bei der Angriffserkennung keine oder vorerst keine Berücksichtigung finden, ist das zu dokumentieren und zu begründen
- Erfassung und Analyse von Systemprotokolldaten und Netzwerkprotokolldaten
- Aktives Sammeln und systematisches Auswerten von Angriffsinformationen für die automatische Angriffserkennung und das Schwachstellenmanagement
- Ausreichend fachkompetentes Personal für die Analyse der Angriffsmeldungen
- Umfänglicher Notfallmanagementprozess (Reaktion)

1.3 Bestandteile eines Systems zu Angriffserkennung

Basierend auf der Beschreibung der OH kann man ein System zur Angriffserkennung in folgende Bestandteile aufgliedern:

Datenerfassung (Protokollierung)

- Die Erfassung relevanter Protokolldaten der betreffenden Systeme und Netzwerke, die Aufschluss über einen Cyberangriff geben können

Detektion

- Die Durchsuchung der Protokolldaten nach geeigneten Hinweisen auf sicherheitsrelevante Ereignisse, wie mögliche Angriffe oder Schwachstellen

Reaktion

- Der angemessene Umgang mit entdeckten sicherheitsrelevanten Ereignissen

1.4 Wie geht man so ein Thema an?

Der Umfang eines solchen Systems, bei dem technische Werkzeuge lediglich ein Bestandteil sind, wird gerne unterschätzt. Auch ohne die Vorgabe der OH beginnt man ein solches Vorgehen mit einer Planung, aus der die erforderlichen Werkzeuge und deren Betriebsmodell hervorgehen.

Da es in jedem Fall schon vorhandene Protokollierungs- und Erkennungsmaßnahmen gibt, lohnt es sich vorher immer, sich in einer GAP-Analyse einen Überblick über den Umfang der Planung und der umzusetzenden Maßnahmen zu verschaffen. Oft ist dann schon absehbar, ob ein Berater hinzugezogen werden soll oder welche Optionen beim Betrieb der Werkzeuge in Frage kommen.

1.4.1 Vorgehensweise einer Planung

- Prüfung aller relevanten Datenquellen (Systeme und Netzwerke) und zu erfassenden Daten anhand des Risikomanagements (Angriffsvektoren, Eintrittswahrscheinlichkeiten, Schadenshöhen) und der Netzwerkstrukturpläne
- Prüfung der zentralen Auswertbarkeit der Daten
- Festlegung von entsprechenden Speicherdauern und entstehenden Speichervolumen
- Beachtung der Datenschutz-Grundverordnung – DSGVO und Betriebsverfassungsgesetz – BetrVG Anforderungen
- Festlegung der Erkennungsmethoden anhand der Angriffsvektoren
- Festlegung eines Prozesses für die systematische und regelmäßige Erfassung und Integration von Angriffsdaten in die Erkennungsmethodik
- Festlegung des gewünschten Betriebsmodells (Leistungen selbst erbringen gegenüber zukaufen). Bei der Nutzung von Dienstleistern, Definition der Schnittstellen
- Prüfung und ggf. Ergänzung vorhandener Notfallmanagement Prozesse

1.4.2 Vorgehensweise Umsetzung

- Abhängig vom Betriebsmodell, Auswahl der Werkzeuge bzw. Dienstleister
- Aufbau der erforderlichen Personalorganisation
- Implementierung der Prozesse
- Implementierung eines Kontinuierlicher Verbesserungsprozesses – KVP – Ein System zur Angriffserkennung erfordert im Betrieb eine kontinuierliche Verbesserung, um effizient und wirksam zu funktionieren
- Durchführung von Übungen zur Feststellung und Verbesserung der Wirksamkeit

1.4.3 Make or Buy Entscheidung

Je nach Auslastung des Informationssicherheitsverantwortlichen (ISB) ist der Einsatz eines Beraters bei der Planung eine hilfreiche Komponente. Es ist ratsam hierbei darauf zu achten, dass idealerweise Erfahrung für genau diese Tätigkeit und ein entsprechender Hintergrund (ISMS für Betreiber des entsprechenden Sektors) vorhanden ist.

Bei der Umsetzung bietet sich der Einsatz von Dienstleistern für kleine und mittelständische Betreiber an, da im Regelfall das vorhandene Personal in anderen Aufgaben gebunden ist. Hinzu kommt, dass der Aufbau einer erforderlichen Personalorganisation weder wirtschaftlich sinnvoll noch kurzfristig umsetzbar ist.

Hier stellt sich die Frage des Betriebsmodells. Soll der Dienstleister die Überwachungssysteme lediglich betreiben, heißt sich um die Verfügbarkeit und Aktualität aller Komponenten kümmern. Oder soll der Dienstleister die Alarme und Meldungen analysieren. Möglicherweise soll er die Leistung ganzheitlich erbringen und die dafür nötigen Komponenten mitbringen. Letzteres hat den Vorteil, dass die Verantwortlichkeiten damit eindeutig festgelegt werden.

Wichtig ist, dass die erhobenen Daten aus der Leittechnik diese nicht verlassen. Das heißt, Datenverarbeitung und Datenhaltung sollte nur innerhalb derselben Infrastruktur erfolgen. Der Einsatz eines Dienstleisters erfolgt dann über sichere (Verschlüsselung, Multi-Faktor-Authentisierung) Fernzugriffsverfahren. So führt eine Kompromittierung beim Dienstleister nicht automatisch dazu, dass die Leittechnikdaten im Darknet wiederzufinden sind.

1.5 Werkzeuge und Methoden

1.5.1 Intrusion Detection System (IDS)

Ein IDS ist ein Werkzeug, das Netzwerkdaten aufnimmt und nach Mustern (auch oft Signaturen genannt) von Angriffen durchsucht. Es kann ebenso genutzt werden, um Abweichungen von bestimmten Kommunikationsparametern (Datenmenge, Zeit, Kommunikationspartner, etc.) zu alarmieren. Abhängig davon, ob der Datenverkehr an einer Netzwerkkomponente (z.B. einem Netzwerk-Switch) ausgeleitet wird oder innerhalb eines Systems (z.B. eines Servers) spricht man von einem Netzwerk-IDS (NIDS) oder einem Host IDS (HIDS).

1.5.2 Logmanagement / SIEM

Ein Logmanagement ist ein zentrales IT-System, das Systemprotokolldaten sammelt, normalisiert und zur Auswertung bereitstellt. Diese Auswertung kann manuell oder automatisch erfolgen. Eine umfangreich automatisierte Suche nach Sicherheitsereignissen und deren Alarmierung wird SIEM System genannt. Mögliche Sicherheitsereignisse sind zum Beispiel eine große Anzahl von Fehlanmeldungen in einer kurzen Zeitspanne. Hier könnte ein Cyberangriff vorliegen.

Neben Systemprotokolldaten können auch Netzwerkprotokolldaten von einem IDS in ein SIEM System zur Speicherung und weiteren Analyse geleitet werden. Sowohl System- als auch Netzwerkprotokolldaten an einer Stelle auswerten zu können, ermöglicht eine umfangreichere Datenanalyse und damit ein besseres Lagebild.

Nachdem eine Verhaltensauffälligkeit in den System- oder Netzwerkdaten erkannt wurde, gilt es den Kontext zu ermitteln. Liegt ein Angriff oder ein Benutzerfehler vor? Dazu braucht es eine hochflexible automatisierbare Suchmaschine, mit der effizient analysiert werden kann. Es wird zum Beispiel danach gefragt, wann von wo nach wo kommuniziert wurde und ob es Ähnliches auch an anderer Stelle oder zu einer anderen Zeit gegeben hat.

Diese Informationen helfen dem Analysten schnell eine Aussage über die Relevanz und Dringlichkeit eines Alarms zu treffen und angemessene Maßnahmen bei der Behandlung zu veranlassen.

1.5.3 Security Analyst – Nebenjob oder Beruf

IDS, Logmanagement und SIEM sind Expertenwerkzeuge mit einer kryptisch anmutenden Bedienoberfläche (Bild 3). In den Händen erfahrener Spezialisten können damit innerhalb kürzester Zeit die erforderlichen Zusammenhänge hergestellt werden (Bild 4). Dabei ist die Kompetenz der Analysten allerdings weit wichtiger als das Analysewerkzeug, da oftmals ohne die richtige Frage nicht auf eine klärende Antwort gehofft werden kann.

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

Oft müssen Analysten komplexe Kommunikationsdatenmitschnitte mithilfe von Suchwerkzeugen interpretieren (Bild 5). 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.

Aus diesem Grund ist das ausreichende Vorhandensein von fachkompetenten Analysten eine explizite Anforderung der OH.

Der kryptische Eindruck entsteht durch die Flexibilität, mit der bei der Analyse den vielen Möglichkeiten eines Cyberangriffs begegnet werden muss. Manche Softwarehersteller versuchen durch stark vereinfachte Benutzerschnittstellen Expertenwerkzeuge auch an Nichtexperten zu verkaufen. Sie erwecken damit den Eindruck, dass dadurch die Leitwarte ohne weiteren Personal- und Know-how Aufbau zum Security Operation Center werden kann. Derartigen Vereinfachungen sollte man mit großer Vorsicht begegnen, da sie im Regelfall bedeuten, dass durch den reduzierten Informationsumfang auch die Leistungsfähigkeit massiv beschnitten wird.

1.5.4 Aufgaben eines SOC

Ein Security Operation Center – SOC ist eine Abteilung, von der aus die Werkzeuge zur Angriffserkennung betrieben werden. Hier findet die Analyse der Meldungen statt und die sicherheitsrelevanten Ereignisse werden

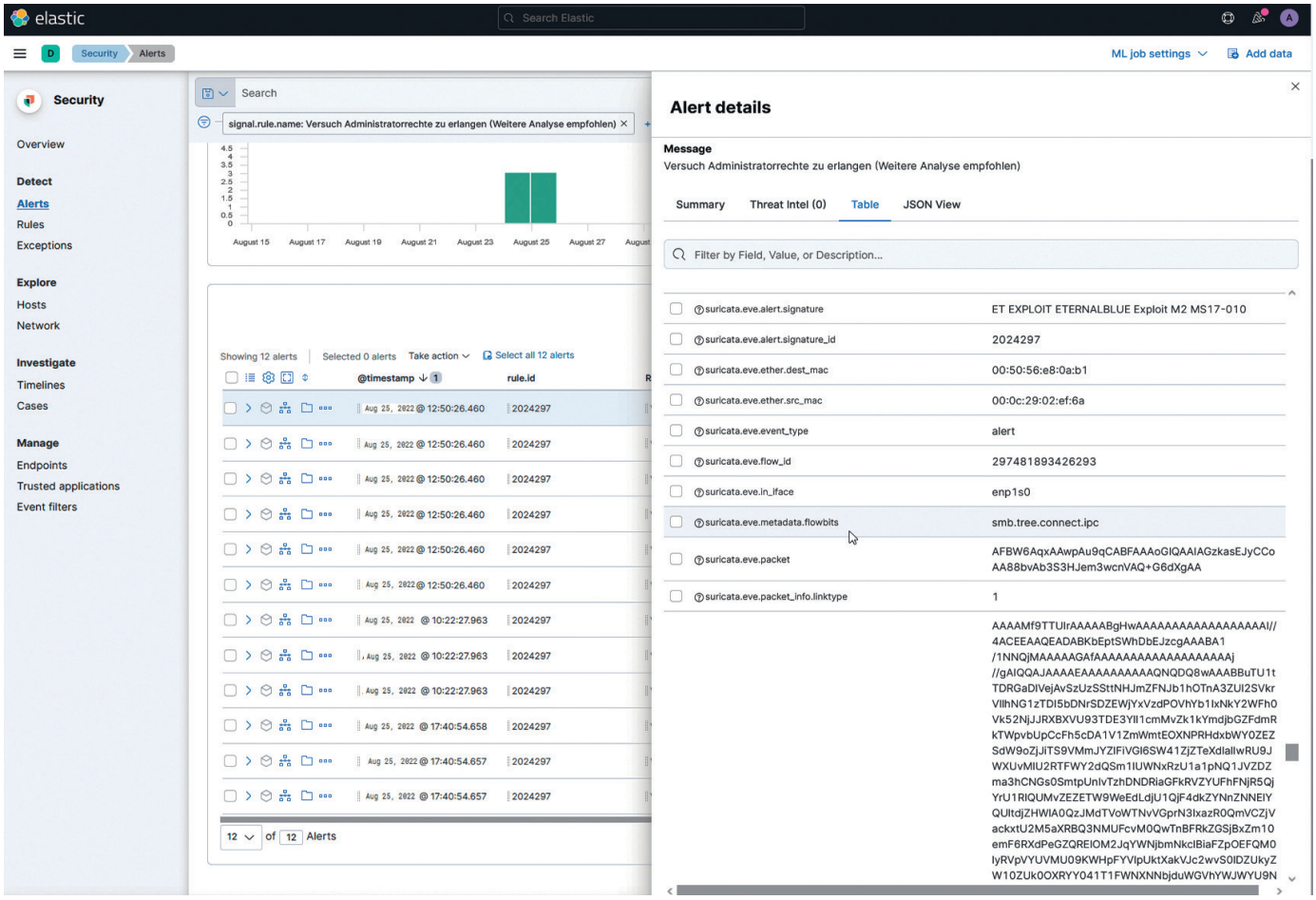

Bild 3. Alarm einer Angriffserkennungssoftware mit vielen Zusatzinformationen.

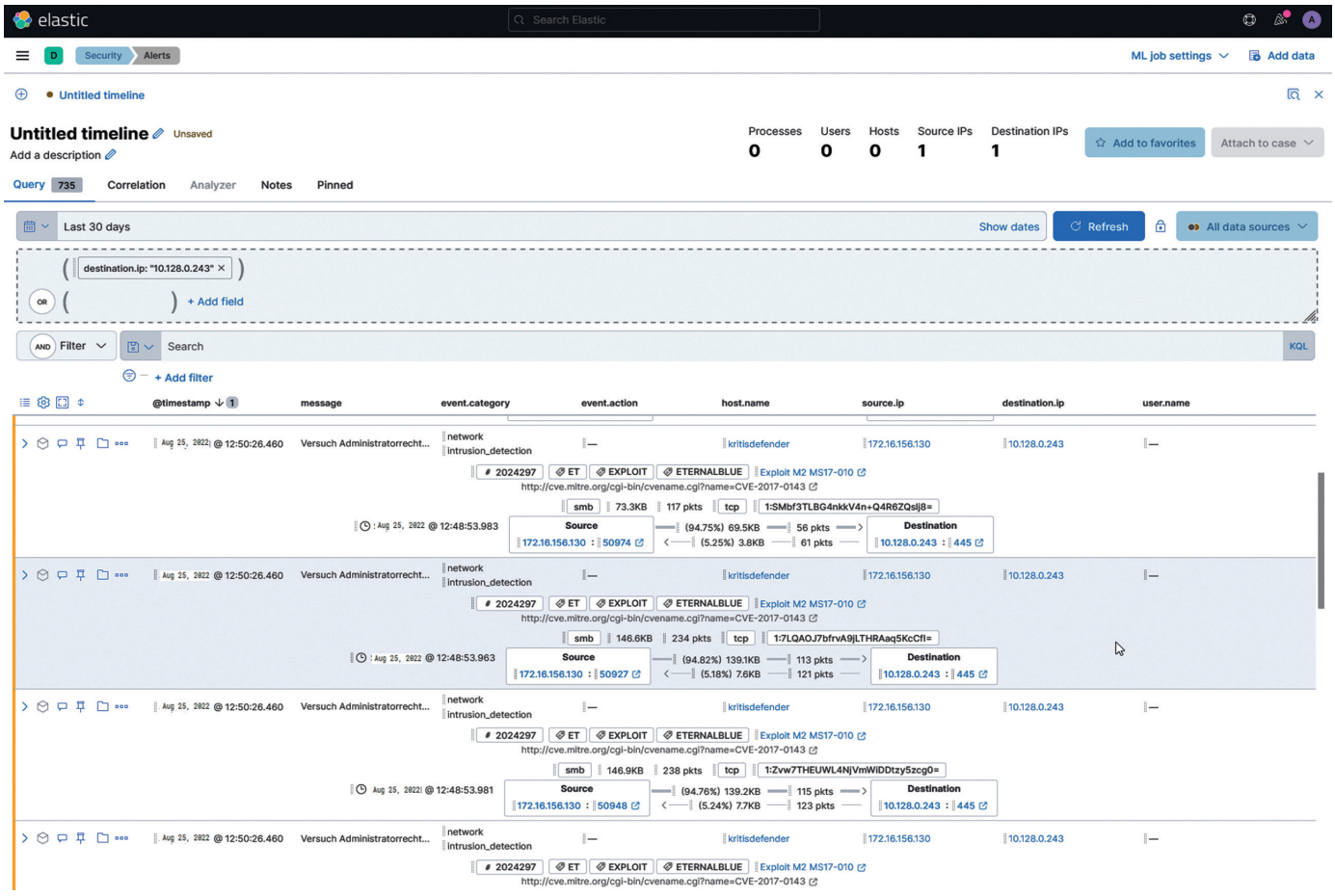

Bild 4. Kontextanalyse (timeline) eines Alarms mit Abfragewerkzeugen.

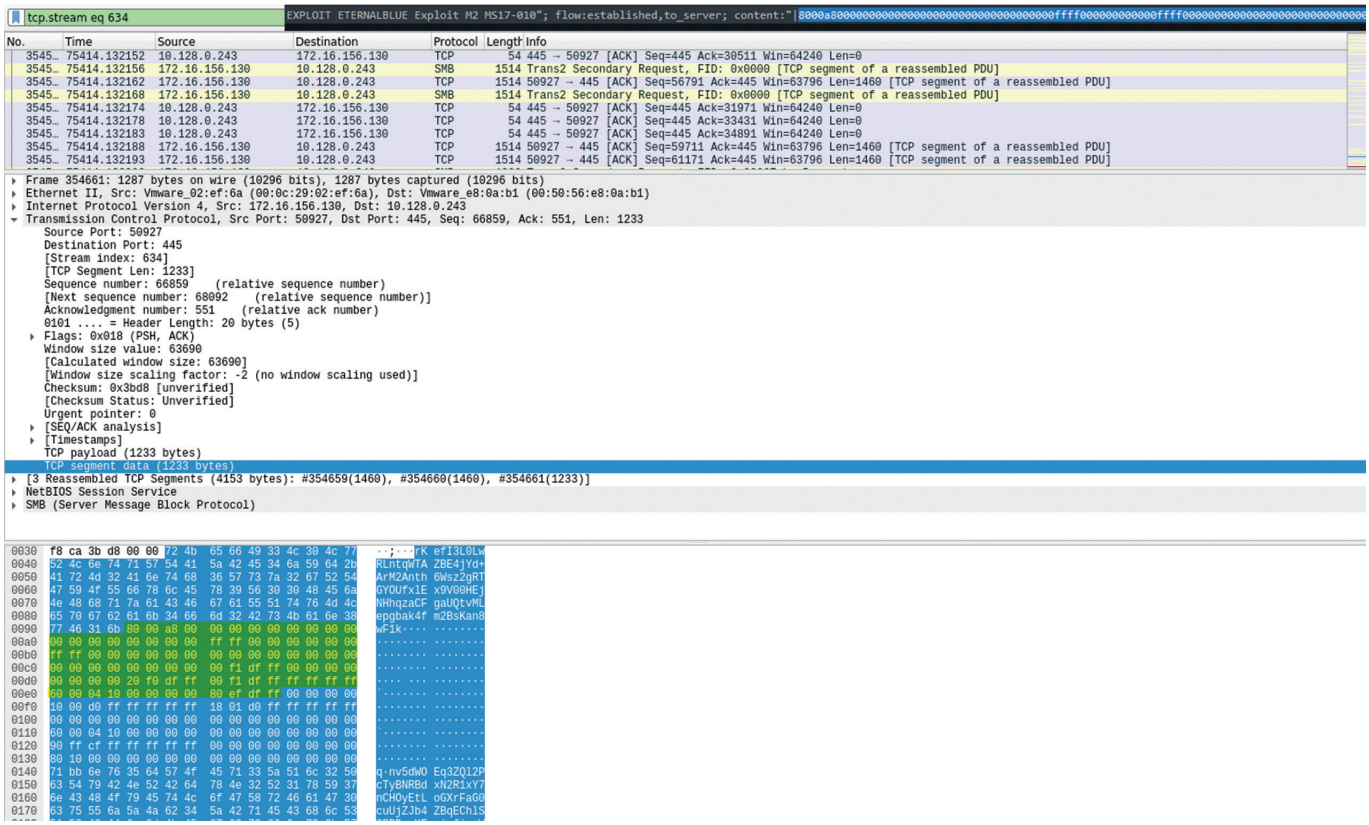

Bild 5. Auswertung von Rohdaten des Netzwerkverkehrs zur Erkennung eines Angriffs.

festgestellt. Je nachdem, was als sinnvoll für die Organisation betrachtet wird, betreibt diese Abteilung möglicherweise auch Systeme für die Netzwerksicherheit (Firewalls) oder andere IT-Security Systeme, wie zum Beispiel Anti Virus Programme. Der Vorteil eines Teams ist die Möglichkeit eines Qualitätsmanagements dieser Leistung und die Gewährleistung einer Verfügbarkeit. Das erfordert eine Mindestgröße an Mannschaft und verursacht damit gleichzeitig erhebliche Kosten. Deshalb entscheiden sich kleinere und mittlere Betreiber im Regelfall dazu, das Team eines Dienstleisters mitzubenutzen.

1.5.5 Erkennungsmethoden: Mustererkennung vs. Anomalieerkennung

Bei der Erkennung von sicherheitsrelevanten Ereignissen 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 (muster- oder signaturbasierte Verfahren) oder nach Abweichungen (Anomalien erkennende Verfahren) von einem Normalzustand (Baseline). Beide Verfahren haben unterschiedliche Eigenschaften. Je nach Einsatzzweck können diese von Vor- und Nachteil sein. Beispielsweise erzeugen rein auf Anomalie Erkennung basierende Werkzeuge in Netzwerken mit IT- und OT-Protokollen auch ohne jeden Angriff kontinuierlich eine Unmenge von Meldungen. Derartigen Netzwerkverkehr findet man in vielen Leittechniknetzen vor. Diese Anomalien müssen dann aufwendig weiter qualifiziert werden, um mögliche Angriffsinformationen zu identifizieren. Dies kann beim Betreiber aufgrund von Zeitmangel bei der Analyse schnell zu einer viel zu umfangreichen Baseline führen, deren Folge der Verlust der Wirksamkeit der Angriffserkennung ist. Ärgerlicherweise erfolgt das unbemerkt und hat noch den trügerischen Nebeneffekt, dass danach der Betriebsaufwand sinkt. Deshalb sollte der Systemzweck und die zu überwachende Umgebung die Methode bestimmen und nicht andersherum.

1.5.6 Besondere Anforderungen von OT/Prozessleittechnik

In vielen Leittechnik-Netzen ist der Einsatz von Mustererkennung die wirksamere Methode, da dort IT typische Systeme und Komponenten betrieben werden, wie zum Beispiel Active Directory und IT-Protokolle (SNMP, SMB, http, etc.) genutzt werden. Hier wird ein Angreifer in der Regel auf bekannte Verfahren für einen Angriff zurückgreifen. Ein ausschließlich auf Anomalie Erkennung basierendes Verfahren würde hier wahrscheinlich große Mengen von falsch-positiven Alarmen erzeugen – eben Anomalien. Außerdem lässt sich die Qualifizierung eines Alarms zu einem Angriffsverfahren und damit auch die Festlegung der Kritikalität und Reaktion mit einem musterbasierten Verfahren viel einfacher und schneller durchführen. Darüber hinaus werden in üblicher Kommunikation, also in der Baseline, gut versteckte Angriffe von einem auf Anomalie Erkennung basierenden Verfahren nicht bemerkt.

Aus diesem Grund ist in der OH auch ein aktives Beschaffen, Auswerten und Anwenden (bedeutet Umsetzung in Erkennungsmuster) von Angriffsinformationen gefordert. Die Erkennung von Anomalien hilft zusätzlich, wie beispielsweise durch die Alarmierung unbekannter Kommunikationspartner.

In Prozessnetzen mit ausschließlicher Leitsystemprotokollkommunikation (z.B. IEC 60870-5-104 [5]) ist dann oftmals die Erkennung von Anomalien das einzig mögliche Verfahren, um Missbräuche zu erkennen. Allerdings ist hier ein gutes Verständnis des Prozesses auf Kommunikationsprotokollebene erforderlich, um die Baseline zu formulieren und gegebenenfalls anzupassen.

Das bedeutet, die vom Betreiber eingesetzten Systeme können im Idealfall beide Verfahren.

1.5.7 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 sicherheitsre#levant identifiziert wird, sollte sie aus der Alarmierung ausgenommen werden. Aber eben nur da. Ansonsten wird damit mit wenigen Handgriffen das Angriffserkennungssystem unwirksam gemacht. Dieses kontinuierli-

che Tuning ist ein wichtiger Bestandteil der Betriebsarbeit.

1.5.8 Rückwirkungsfrei oder besser doch nicht?

Als rückwirkungsfrei werden Werkzeuge bezeichnet, die eine unidirektional erzeugte Kopie des Datenverkehrs analysieren. 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 (beispielsweise bei SolarWinds, Kazeya), ebenso wie auch aufwendig von allen anderen Netzen getrennte Offline-Netzwerke, eine sehr wirksame Sicherheitsmaßnahme.

Derselbe Vorteil gilt insbesondere dann, wenn bei der Angriffserkennung ein Dienstleister beteiligt ist. Durch die Rückwirkungsfreiheit ist selbst eine Kompromittierung des Dienstleisters zunächst nicht gravierend.

Das bedeutet für das Werkzeug aber auch, dass Softwareagenten auf den Endgeräten, nicht möglich sind. Ebenso wenig erlaubt eine rückwirkungsfreie Verbindung automatisierte Verbindungsabbrüche bei erkannten Verhaltensbesonderheiten, wie zum Beispiel bei einem Intrusion Prevention System (IPS). In der Prozessleittechnik ist das aber auch weder ratsam noch erwünscht.

1.5.9 Vor- und Nachteil von automatischen Verfahren zur Abwehr

Viele IT-Sicherheits-Software bieten eine automatisierte Reaktion auf bestimmte Vorkommnisse an. Beispielsweise ist es eine Grundfunktion von Firewall Systemen, 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 beispielsweise der Leit- und Fernwirktechnik, sollte eine wirksame Angriffserkennung dann deutlich sensibler erfolgen. Hier erfordert eine eindeutige Erkennung dann oft weitergehende Untersuchungen. Auch die Entscheidung über weitere Schritte (beispielsweise das Umschalten einer Anlage auf manuellen Betrieb) mit all ihren Konsequenzen sollten unbedingt bei den erfahrenen Mitarbeitern des Anlagenbetreibers liegen und nicht bei IT-Systemen.

Deshalb weist die OH darauf hin, dass in begründeten Fällen auf eine automatische Reaktion verzichtet werden darf.

1.5.10 Unterschiede zwischen proprietärer Software und Open Source

Im Bereich der Betriebssysteme hat das Open Source System Linux nahezu alle anderen Systeme bis auf den Platzhirsch 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 ergibt sich daraus, dass der Programmcode (Source) bekannt (Open) ist. Allerdings ist für ihren Betrieb und die Nutzung 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.

1.6 Umgang mit einem Cyberangriff

Nach der Identifikation eines Cyberangriffs ist vor allem ein überlegtes Handeln erforderlich, um den entstandenen Schaden möglichst weit einzugrenzen (Bild 6). Dabei macht sich die Vorbereitung auf diesen Fall intensiv bemerkbar:

- Wirksamer Sicherheitsvorfallprozess. Hier fordert die OH die Mindestanforderungen des IT-Grundschutz Bausteins DER.2.1: Behandlung von Sicherheitsvorfällen [6]
- Wirksames Notfallmanagement (z.B. nach BSI 200-4 [7])
- Vereinbarte Partnerschaften (z.B. Rahmenvertrag und Arbeitsteilung mit Incident Response Dienstleistern)
- Regelmäßig geübtes gemeinsames Vorgehen aller Beteiligten

1.7 Angriffserkennung als Dienstleistung

1.7.1 Angriffserkennung braucht Mitarbeiter und 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 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

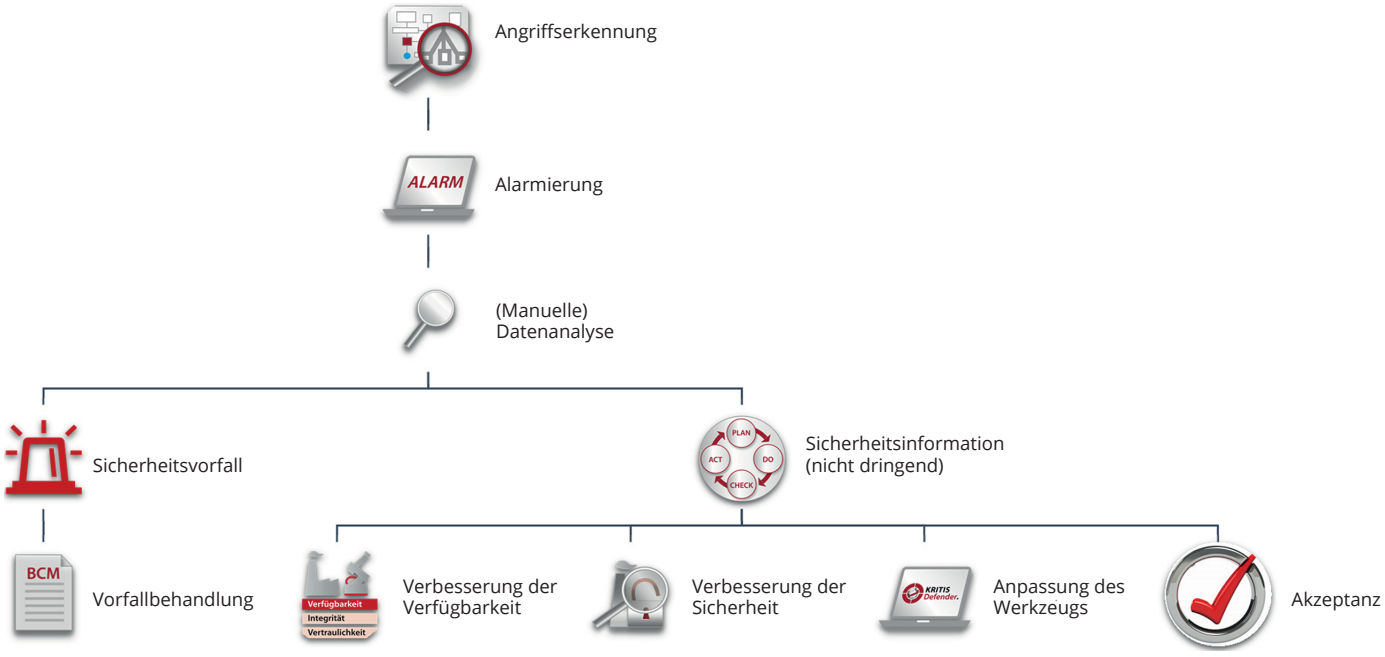

Bild 6. Prozessabbildung Angriffserkennung.

Dienstleister leichter geeignetes Personal finden und ausbilden können.

1.7.2 Aufgabenteilung bei der Nutzung eines Dienstleisters

Die Annahme, dass der Dienstleister die Angriffserkennung komplett übernimmt, ist insbesondere in komplexen Leittechnikumgebungen unrealistisch. Das dafür erforderliche Detailwissen kann auch der beste Dienstleister nicht vorhalten, beispielsweise welches System sich hinter welcher Adresse verbirgt und welcher Techniker gerade an welchem System arbeitet. Aus diesem Grund ist es absolut essenziell den Anlagenbetreiber in die Analyse miteinzubeziehen, um dann zu entscheiden, ob es ein Angriff oder eher eine ungeplante Entstörung ist. Insofern könnten Sie den Dienstleister auch als verlängerte Werkbank oder die Zusammenarbeit neudeutsch als Hybrid betrachten.

1.7.3 Vorteile beim Know-how Aufbau

Manche Verantwortliche wählen bewusst den Eigenbetrieb, weil sie fürchten, dass sie sonst weniger Know-How in der eigenen Organisation aufbauen können. Die regelmäßige Zusammenarbeit mit den Analysten eines Dienstleisters hat tatsächlich die gegenteilige Wirkung – Der Know-how Aufbau beim Kunden findet erheblich schneller statt. Das Wissen zu der überwachten Anlage, deren Schwachstellen und möglichen IT-Bedrohungen wird laufend größer. Im Vergleich zum Eigenbetrieb muss sich dieses Wissen aber nicht autodidaktisch angelernt werden. Stattdessen werden die Mitarbeiter in konkrete, praktische Beispiele einbezogen. Erfahrene Analysten eines guten Partners erklären ihre Beobachtungen und Handlungsvorschläge verständlich und beraten auf Augenhöhe.

Die fachliche Kompetenz und Vermittlungsfähigkeit der Analysten sollten für Betreiber wichtige Faktoren bei der Auswahl eines Dienstleisters sein.

1.7.4 Schnittstellen zum Dienstleister

Üblicherweise liegt die Planungsverantwortung beim ISB. Je nach Umfang und Verfügbarkeit kann sich dieser durch externe Beratung verstärken.

Die Umsetzung von Protokollierung und Detektion bis hin zur Alarmierung kann ein Dienstleister vollumfänglich übernehmen. Je flexibler die Werkzeuge des Dienstleisters sind, umso besser können bestehende Systeme, wie beispielsweise ein bereits vorhandenes Logmanagementsystem integriert werden. Dadurch können Kosten gespart und die Integration in vorhandene Prozesse beim Kunden erhöht werden.

Der Teilbereich Reaktion erfordert einen Prozess in der Organisation des Betreibers. Bei der Erstellung ist sowohl die Verwendung von frei verfügbaren Standards [siehe 6, siehe 7], als auch der Einsatz eines erfahrenen Beraters eine große Hilfe. Zusätzlich ist die fachliche externe Unterstützung von einem kompetenten Analysten bei einem Sicherheitsvorfall ein erheblicher Mehrwert.

Sollte der Sicherheitsvorfall nicht durch die vorstehenden Maßnahmen unmittelbar eingedämmt werden können, ist in den meisten Fällen ein Incident Response Dienstleister erforderlich. Dieser Fall ist in der Regel sehr personal- und kostenaufwendig, aber bisher sehr selten. Hier lohnt sich der Abschluss eines Rahmenvertrags mit Reaktionszeiten und Kostenrahmen, um nicht in höchster Not jedes Angebot annehmen zu müssen.

1.8 Unterschiedliche Dienstleistungsmodelle – Was passt für wen?

Aus diesem Grund ist es wichtig, dass Anlagenbetreiber bei der Wahl des Dienstleisters darauf achten, dass die Leistung zu ihren Anforderungen passen:

- Sind die eingesetzten Werkzeuge auf den Einsatz in der jeweiligen Anlage zugeschnitten?
- Können vorhandene Systeme (Logmanagementsystem, etc.) integriert werden?
- Was passiert mit den Daten? Wenn die Daten beim Dienstleister verarbeitet werden (z.B. auch in dessen Ticketsystem) stellt dieser ein zusätzliches Sicherheitsrisiko dar.
- Wie umfangreich, aktuell und spezifisch sind die angewendeten Angriffsmuster?
- Wie spezifisch (welche Parameter werden berücksichtigt) ist das Baselining Verfahren, wenn Anomalie-Erkennung eingesetzt wird?
- Wie gut werden die Werkzeuge kontinuierlich auf die Anforderungen angepasst?
- Arbeiten die Analysten des Dienstleisters mit einem diensthabenden Mitarbeiter beim Anlagenbetreiber auf Augenhöhe zusammen (Sprache, fachliche Qualifikation, Verständnis der Anlage)?

1.8.1 Near- und Offshoring – Kostenoptimierung der großen Dienstleister – nicht ohne Nebenwirkungen

Große IT-Dienstleister benötigen zur Selbstverwaltung komplexe Prozesse und haben hohe Verwaltungskosten. Um dennoch wettbewerbsfähig anbieten 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 wiederum Auswirkungen auf die Leistungsqualität, beispielsweise durch einen andauernd wechselnden Ansprechpartner, der den Betreiber und seine Umgebung nicht ausreichend kennt. Gerade bei IT-Sicherheitsleistungen, bei denen das Wissen über die überwachte Anlage entscheidend ist, spielt das eine große Rolle.

1.9 Angriffserkennung kann auch ohne Angriffe sehr positive Nebenwirkungen haben

Die heute üblichen Sicherheitsmechanismen (beispielsweise Firewalls) wehren im Regelfall die meisten Angriffsversuche ab. Deshalb sind Angriffe in Leittechnikumgebungen eher selten. Warum sollten Kunde und externe Analysten dann trotzdem regelmäßig miteinander interagieren?

Wirksam betriebene Angriffserkennungssysteme können viel mehr als nur Angriffe erkennen. Einerseits werden Schwachstellen sichtbar, wie beispielsweise unverschlüsselte Passwortübertragungen oder vulnerable Protokollversionen. 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. Das ist allerdings nur dann der Fall, wenn die Analysten derartige Zusammenhänge aus den gesammelten Daten herauslesen und interpretieren können. Ebenso wichtig ist, dass die dabei gefunden Schwachstellen in den regelmäßigen Verbesserungsprozess aufgenommen werden (KVP).

Die OH fordert, dass die im Rahmen der Angriffserkennung bemerkten Schwachstellen unmittelbar in den dokumentierten Schwachstellenmanagementprozess des Betreibers aufgenommen werden.

1.10 Zusammenfassung und Erfahrungen des Autors

Unter Berücksichtigung aller genannten Punkte ist der Aufbau und Betrieb eines Systems zur Erkennung von Cyberangriffen in der Produktionsumgebung eines Versorgungsunternehmens sinnvoll und notwendig. Das alles aus eigener Kraft zu tun und dauerhaft autark technisch, wie personell zu bewerkstelligen ist nur ab einer ausreichenden Unternehmensgröße wirtschaftlich machbar, völlig abgesehen von der Herausforderung geeignetes Personal zu finden und dauerhaft zu halten. Alle anderen Versorger sind gut beraten sich mit geeigneten Dienstleistern zu verstärken.

Wichtig dabei ist Augenhöhe und Flexibilität, da sich heute noch gar nicht absehen lässt, welche Anforderungen hier in der

Zukunft entstehen. Hohe Investitionskosten und langfristige Bindungen stehen hier eher im Weg. Das stellt einen Paradigmenwechsel zu früheren Systemeinführungen dar.

Die in diesem Artikel beschriebene Erkenntnis hat der Autor mit dem eigenen Unternehmen, einem Spezialdienstleister für Informations- und IT-Sicherheit von Versorgern, bei seinen Kunden genau so erfahren. Die Idee, ein System zur Angriffserkennung für die Leittechnik zu entwickeln, entstand aus den regelmäßig gefundenen Schwachstellen bei Penetrationstests in Kundenumgebungen. Die daraufhin erstellte Software führte bei Pilotkunden nach anfänglicher Euphorie, dann aber sehr schnell zu der Feststellung, dass weder Zeit- noch Know-how da war, um ein solches Werkzeug wirksam zu betreiben.

Aus dieser Erfahrung entstand dann eine Dienstleistung, die an den Anforderungen kleiner und mittlerer Versorger und Erzeuger ausgerichtet ist. Hierbei standen nicht nur die technischen Leistungsmerkmale im Vordergrund, sondern auch die Kundenforderung, dass die gesamten Betriebskosten für Angriffserkennung in gesunder Relation zu der geschützten Infrastruktur stehen müssen. An dieser Stelle zeigt der Einsatz von Open Source Werkzeugen seine große Stärke. Neben dem regelmäßigen Dialog mit den Nutzern hat die enge Zusammenarbeit mit dem BSI sehr geholfen, gesetzliche Anforderungen abzubilden. Im Rahmen einer Usergroup werden regelmäßig die Entwicklungsplanungen abgestimmt und neue Leistungsmerkmale pilotiert. Bei all dem ist der Einsatz von agilen Verfahren wie Scrum [8] und entsprechenden Werkzeugen wie GIT [9] und Methoden wie continuous integration und continuous deployment (CI/CD) [10] essenziell.

Literaturverzeichnis

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

[2] *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 (https://t1p.de/vgbe-ej-202209-SJ1).

[4] Veröffentlichung OH zum Einsatz von SzA https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=8

[5] Wikipedia https://de.wikipedia.org/wiki/IEC_60870 (https://t1p.de/vgbe-ej-202209-SJ3).

[6] BSI *IT-Grundschutz-Bausteine Edition 2022*. https://www.bsi.bund.de/dok/531534 (https://t1p.de/vgbe-ej-202209-SJ4).

[7] BSI *Standard 200-4* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4_CD.pdf?__blob=publicationFile&v=3 (https://t1p.de/vgbe-ej-202209-SJ5).

[8] *Scrum ist ein Vorgehensmodell des Projekt- und Produktmanagements* https://www.scrum.org/ (https://t1p.de/vgbe-ej-202209-SJ6).

[9] Git ist eine freie Software zur verteilten Versionsverwaltung von Dateien, die durch Linus Torvalds initiiert wurde https://git-scm.com/ (https://t1p.de/vgbe-ej-202209-SJ7).

[10] Rossel, Sander (October 2017). *Continuous Integration, Delivery, and Deployment*. Packt Publishing. ISBN 978-1-78728-661-0.

(in Klammern: jeweiliger Kurzlink

Quellen, Bilder

Bilder 1, 3, 4, 5, 6: ausecus GmbH. Bild 2: BSI

vgbe energy journal
Deilbachtal 173
45257 Essen
Germany

t +49 201 8128-300
e pt@vgbe.energy