Neue Anforderungen IT-SIG 2.0 für Leittechnik

Angriffserkennung wirksam und effizient umsetzen

Angriffserkennung in kritischen Infrastrukturen ist seit dem IT-SiG 2.0 ein viel diskutiertes Thema. Es gibt erhebliche Unterschiede bei den Vorstellungen, welche Werkzeuge und Betriebsleistungen erforderlich sind. Gerade für mittelständische Betreiber ist der Einsatz von Dienstleistungen sinnvoll. Sascha Jäger von Ausecus zeigt, welche Werkzeuge für eine wirksame Angriffserkennung erforderlich sind, warum oft eine Dienstleistung 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 Stromverteilnetzen 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 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 ist.

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- oder Nachteil sein. Beispielsweise erzeugen rein auf Anomalie-Erkennung basierende Werkzeuge in Netzwerken mit IT- und OT-Protokollen, wie sie heute bei nahezu jedem Kunden vorherrschen, auch ohne jeden Angriff kontinuierlich eine Unmenge von Meldungen, die dann aufwendig weiter qualifiziert werden müssen. Deshalb sollte der Systemzweck und die zu überwachende Umgebung die Auswahl der Tools bestimmen und nicht andersherum.

IDS ist nicht gleich IDS

Wenn ein Angriffserkennungssystem in der Prozessleittechnik eingesetzt werden soll, dann sollte dieses auch in der Lage sein, neben bekannten Angriffsverfahren aus der IT auch diejenigen auf Leittechniksysteme und Leittechnikprotokolle (zum Beispiel 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 einmal für eine größere Zufriedenheit und verkauft sich damit besser. Ein trügerischer Vorteil.

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-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 nahen Vergangenheit, bei denen Softwarehersteller für den Angriff missbraucht wurden (zum Beispiel 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, zum Beispiel 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 Platzhirsch Microsoft verdrängt. Auch im Bereich der IT-Sicherheitswerkzeuge sind die Open-Source-Software-Projekte (OSS) im Vormarsch. Durch die großen und internationalen Communities sind sie nicht nur lizenzkostenfrei, sondern auch sehr innovativ und sicher. Grund dafür ist, dass der Programmcode (Source) bekannt (Open) ist. Allerdings ist für deren Betrieb und die Nutzung der oft 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 aus dem mittelständischen Bereich, 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 wird mit wenigen Handgriffen das Angriffserkennungssystem unwirksam gemacht. Dieses kontinuierliche Tuning ist ein wichtiger Bestandteil der Betriebsarbeit.

Werkzeuge zur Datenanalyse werden häufig vergessen

Nachdem eine Verhaltensauffälligkeit im Datenverkehr erkannt ist, gilt es, den Kontext zu ermitteln (War es ein Angriff oder eine Datensicherung?). Notwendig ist dafür eine hochflexible automatisierbare Suchmaschine mit der effizient analysiert werden kann: was wurde wann von wo nach wo kommuniziert und hat es Ähnliches auch an anderer Stelle oder zu einer anderen Zeit bereits gegeben. 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 weitaus wichtiger als das Analysewerkzeug selbst, da sich oft ohne die richtige Frage keine klärende Antwort finden lässt (**Bild 1** und **2**).

Deshalb braucht es erfahrene Spezialisten beim Betreiben

Für effizientes Tuning und Analysieren ist außer 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 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**).

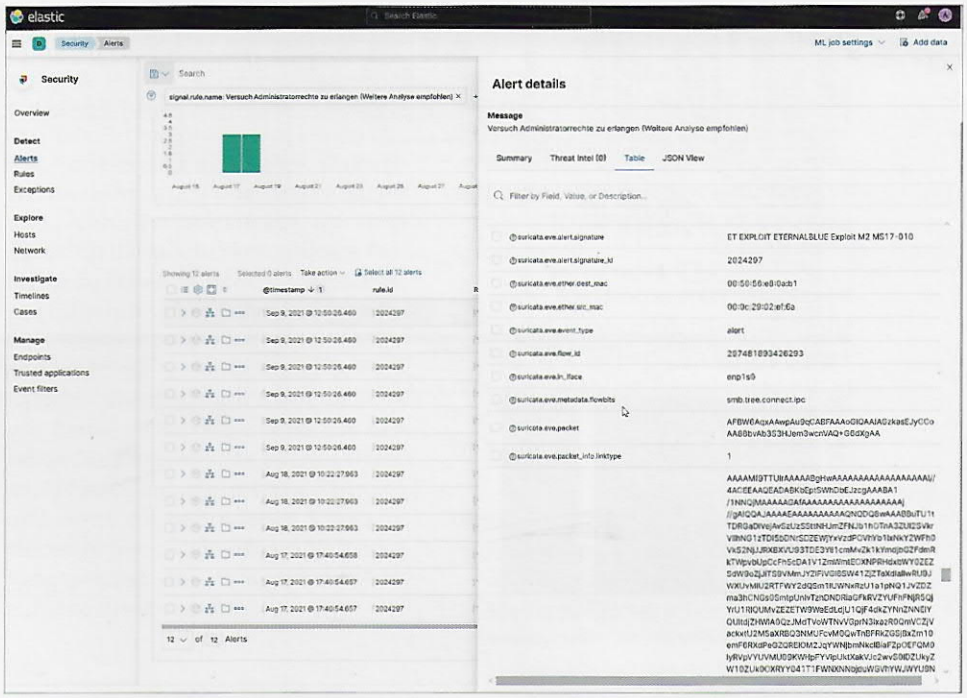

Bild 1. Alarm einer Angriffserkennungssoftware mit vielen Zusatzinformationen

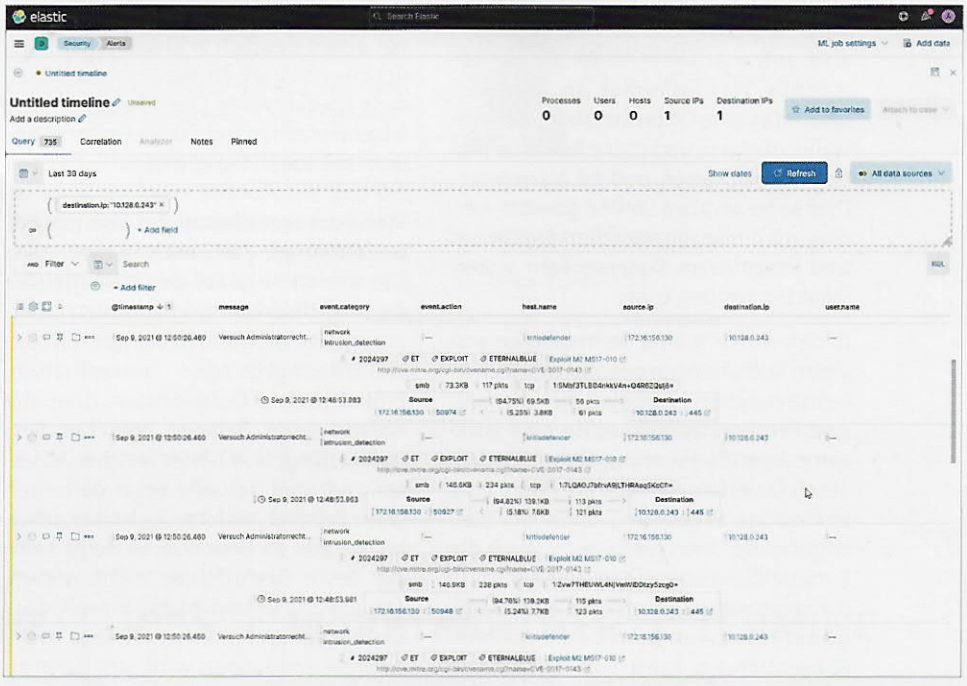

Bild 2. Kontextanalyse (timeline) eines Alarms mit Abfragewerkzeugen

Was ist, wenn ein Angriff identifiziert wurde?

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

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

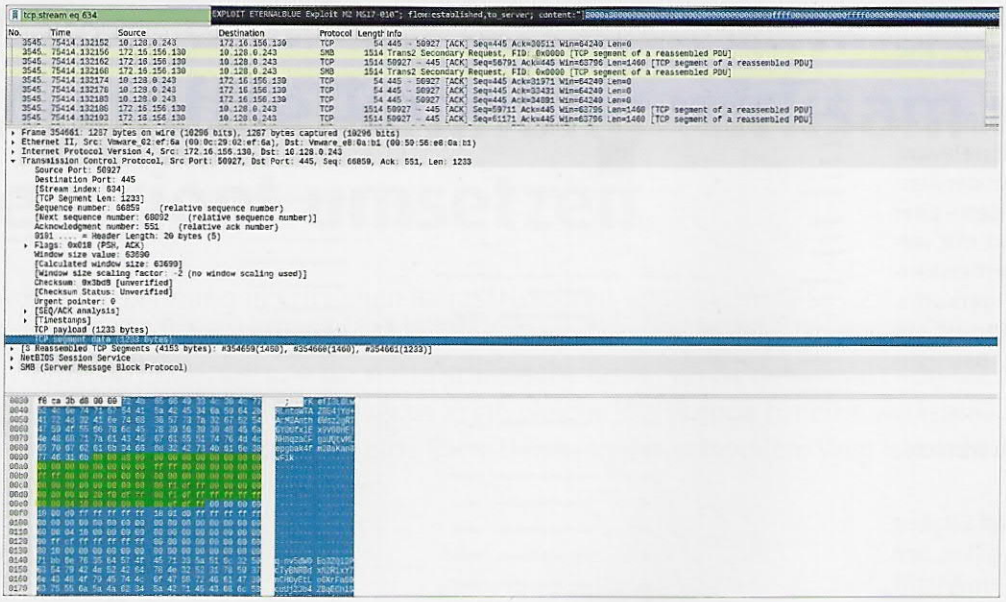

Bild 3. Auswertung von Rohdaten des Netzwerkverkehrs zur Erkennung eines Angriffs

An dieser Stelle kommen häufig die im Folgenden diskutierten Fragen auf.

Warum kann das die Technik nicht von allein?
Viele IT-Sicherheits-Softwares bieten eine automatisierte Reaktion auf bestimmte Vorkommnisse an. Zum Beispiel 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, zum Beispiel die Leit- und Fernwirktechnik, sollte eine wirksame Angriffserkennung dann deutlich sensibler erfolgen. Hier erfordert eine eindeutige Erkennung dann oft weitergehende Untersuchungen. Auch die Entscheidung über die weiteren Schritte (beispielsweise Umschalten einer Anlage auf manuellen Betrieb) mit all ihren Konsequenzen kann von erfahrenen Mitarbeitern erheblich besser getroffen werden als von IT-Systemen.

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 Vorhalten eines Teams aus solchen 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 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 vor allem in komplexen Leittechnikumgebungen unrealistisch. Erforderliches Detailwissen über die Anlage (zum Beispiel: Welches System verbirgt sich hinter welcher Adresse) und über aktuelle Besonderheiten (zum Beispiel: Welcher Techniker arbeitet gerade an welchem System) kann der beste Dienstleister nicht wissen. Aus diesem Grund ist es sinnvoll, dass das Betriebspersonal der Anlage in die Analyse einbezogen wird, um dann zu entscheiden, ob es sich um einen Angriff oder zum Beispiel eine ungeplante Entstörung handelt. Insofern lässt sich der Dienstleister auch als verlängerte Werkbank oder die Zusammenarbeit als hybrid betrachten.

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 – die Mitarbeiter gewinnen kontinuierlich an Know-how. Das Wissen über die Anlage und zu möglichen IT-Bedrohungen wird laufend größer. Im Vergleich zum Eigenbetrieb müssen sich die Mitarbeiter 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 die Mitarbeiter auf Augenhöhe.

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

- Sind die eingesetzten Werkzeuge auf den Einsatz in der betrachteten Anlage zugeschnitten?
- Was passiert mit den Daten? Wenn die Daten beim Dienstleister verarbeitet werden (zum Beispiel auch in dessen Ticketsystem), stellt dies ein zusätzliches Sicherheitsrisiko dar.
- Wie gut werden die Werkzeuge kontinuierlich auf die jeweiligen Anforderungen angepasst? Eine organisatorische Trennung zwischen Entwicklungs- und Betriebsteams hat hier Nachteile.
- Wie gut arbeiten die Analysten des Dienstleisters mit einem diensthabenden Mitarbeiter auf »Augenhöhe« zusammen (Sprache, fachliche Qualifikation, Verständnis der Anlage)?

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 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 wiederum Auswirkungen auf die Leistungsqualität (jedes Mal ein neuer Ansprechpartner, der die 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 sehr positive Nebenwirkungen haben

Die heute üblichen Sicherheitsmechanismen (zum Beispiel 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, 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 zu Störungen führen. Insofern liefert ein Angriffserkennungssystem einen dauerhaften Mehrwert für Sicherheit und Verfügbarkeit – allerdings nur dann, 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 des Anlagenbetreibers aufgenommen werden.

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 großer Unterschied, den ein Auditor hoffentlich eher bemerkt als ein Angreifer.

Die Erfahrungen zeigen, dass ein wirtschaftlicher Eigenbetrieb nur den Betreibern großer Umgebungen im Rahmen eines eigenen Security Operation Centers (SOC) vorbehalten ist. 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 die Ausecus GmbH in den vergangenen Monaten gesprochen hat.

Da sich funktionierende Sicherheit nur in der Praxis zeigt, ist vor allem 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] BSI-Gesetz §8a 1a), BSI-Gesetz §2 9b) www.gesetze-im-internet.de/bsig_2009

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

Sascha Jäger,
Geschäftsführer und Gesellschafter,
ausecus GmbH, Augsburg

>> info@ausecus.com

>> www.ausecus.com