Countdown für Systeme der Angriffserkennung

Ab dem 1. Mai 2023 besteht die Verpflichtung zum Einsatz von Systemen zur Angriffserkennung gemäß dem Gesetzeswortlaut. Konkretere Anforderungen für Betreiber kritischer Infrastrukturen werden zurzeit durch das BSI erarbeitet und in Form einer Orientierungshilfe veröffentlicht. Doch was bedeutet das alles konkret für die Unternehmen und wie können oder sollten sie sich schon jetzt vorbereiten?

Prof. Stefan Loubichi

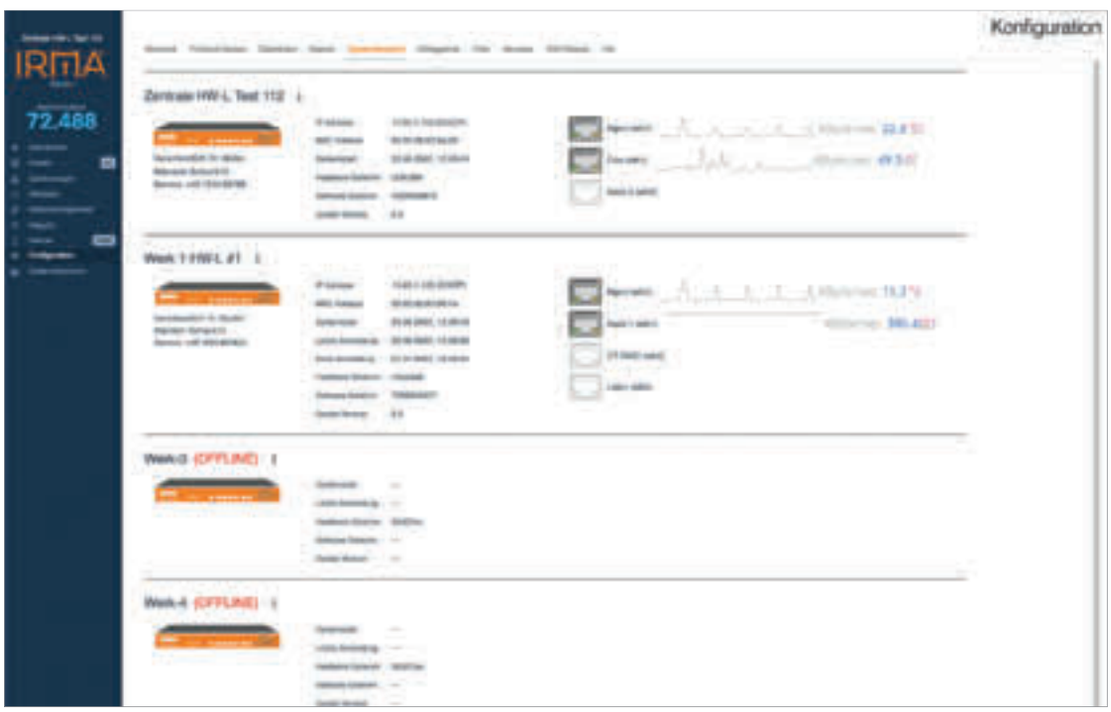

Bild: Videc

Mit der OT-Security-Lösung Irma von Videc werden Automatisierungsnetze überwacht und geschützt

Viele erinnern sich wahrscheinlich noch an die Ende 2021/2022 aufgetretenen kritischen Schwachstellen in Log4J (als CVE-2001-44228 dokumentiert). Durch sie konnten Angreifer ohne Authentifizierung auf Systeme zugreifen, die die Log4J-Bibliothek verwenden, um dort Schadcode auszuführen. Die richtige Lösung für Betreiber kritischer Infrastrukturen wäre damals (und ist es auch noch heute in gleich gelagerten Fällen) das Update aller im Unternehmen existierenden Log4J-Bibliotheken auf die aktuellste Version gewesen. Oftmals wissen die Unternehmen aber gar nicht, welche Applikationen die Bibliotheken nutzen, und ein einmaliges globales Java-Update der Log4J-Bibliothek über die Softwareverwaltung auf Betriebssystemebene reicht hier nicht aus. In der Regel können auch nur die Softwarehersteller, welche die Bibliotheken in die Programme eingebunden haben, das Update vornehmen. Um trotzdem Angriffe zu erkennen, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Arbeitspapier „Log4J: Detektion und Reaktion" zur Verfügung gestellt. Hier wurde allerdings die Anomalieerkennung auf Netzwerkebene als das nach diesseitiger Sicht eindeutig wirkungsvollste Tool vorgestellt. Sicherlich ist das umgehende Patchen noch besser. Aber manchmal ist die zweitbeste Lösung immer noch besser als gar keine Lösung.

Das magische Datum 1. Mai 2023

Gemäß § 8a Abs. 1a BSI-Gesetz sind Betreiber kritischer Infrastrukturen ab dem 1. Mai 2023 auf den Einsatz von Systemen zur Angriffserkennung verpflichtet: „Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und auto-

matisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohung zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen."

Gerade aufgrund der oben geschilderten positiven Erfahrung des BSI mit Angriffserkennungssystemen ist es eher unwahrscheinlich, dass das BSI hier über die Frist hinwegsehen wird, zumal diese Frist nicht in einer Verordnung, sondern in einem Bundesgesetz festgehalten wurde. Für Betreiber kritischer Infrastrukturen im Energiesektor ist neben § 8a Abs. 1a BSI-Gesetz auch noch § 11 (1d) EnWG zwingend zu beachten.

Gemäß § 8a (3) BSI-Gesetz müssen die Betreiber kritischer Infrastrukturen entsprechende Nachweise gegenüber dem BSI vorlegen. Bereits heute hat das BSI darauf hingewiesen, dass ab dem 1. Mai 2023 auch die Ergebnisse der Systeme zur Angriffserkennung inklusive der aufgedeckten Sicherheitsmängel vorzulegen sind. Für die meisten Betreiber kritischer Infrastrukturen aus dem Energiesektor ist hierfür § 11 (1e) die entsprechende Gesetzesgrundlage zur Umsetzung.

Theoretisch existiert bereits ein sehr guter Ansatz durch das BSI-Dokument: „Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen nach § 8 (1) 1 BSI-Gesetz" (Version 1.0a vom 25. Februar 2021). Allerdings bezieht sich dieser 86-seitige Mindeststandard „nur" auf die Informationstechnik des Bundes. Um den Wünschen der Betreiber kritischer Infrastrukturen entgegen zu kommen, hat das BSI ein separates Arbeitsdokument im Entwurfsstadium zum 1. Juni 2022 zur Verfügung gestellt: „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung inklusive Formulare für den Nachweis zu § 8a (1a) BSIG und § 11 (1d) EnWG." Selbst für den Fall, dass diese Orientierungshilfe nicht bis zum 1. Mai 2023 freigegeben sein sollte, wird dies die Betreiber kritischer Infrastrukturen nicht von ihrer Verpflichtung in Sachen Einsatz von Systemen zur Angriffserkennung entbinden. Diese Orientierungshilfe stellt im Übrigen keine verbindliche Vorgabe dar.

Auf jeden Fall zu beachten sind die BSI Bausteine:

- OPS.1.1.4 Schutz vor Schadprogrammen,
- OPS.1.1.5 Protokollierung,
- NET.1.2 Netzmanagement,
- NET.3.2 Firewall,
- DER.1 Detektion von sicherheitsrelevanten Ereignissen,
- DER.2.1 Behandlung von Sicherheitsvorfällen sowie
- Kapitel 2.2 und 2.3 des Mindeststandards des BSI zur Protokollierung und Detektion von Cyber-Angriffen nach § 8a (1) 1 BSIG.

In den Normenreihen der ISO/IEC 2700x sowie der IEC 62443 sind wichtige Anforderungen an Detektion und Reaktion formuliert. Gleichwohl reicht eine Zertifizierung nach einer dieser Normen (in der Regel) nicht aus, um einen entsprechenden Nachweis nach § 8a (1a) BSIG bzw. § 11 (1d) EnWG zu erbringen. Es empfiehlt sich hier stets eine zeitnahe Kontaktaufnahme zum BSI, die gerne bei Fragen weiterhelfen, was im Rahmen von bestehenden Zertifikaten „anerkannt" werden kann.

Unter Bezug auf § 2 (9) 1 BSIG sei darauf verwiesen, dass Systeme zur Angriffserkennung stets auch organisatorische Maßnahmen erfordern, welche bei der Planung der Ressourcenverteilung zu berücksichtigen sind.

Systeme zur Angriffserkennung beziehen sich sowohl auf die IT als auch auf die OT sowie auf weitere Bereiche, wie Rechenzentren oder Embedded-Systeme.

Für zukünftige Prüfungen im Rahmen der branchenspezifischen Sicherheitsstandards (B3S) sei auch darauf verwiesen, dass diese zukünftig Vorgaben für Systeme für Angriffserkennung abdecken müssen. Somit wird ab dem 1. Mai 2023 kein Weg mehr an Systemen zur Angriffserkennung vorbeiführen.

Allgemeine Anforderungen gemäß des Entwurfs der Orientierungshilfe (OH) sind:

- Signaturen von Detektionssystemen müssen immer aktuell sein,
- Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten müssen fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden,
- alle zur Angriffserkennung erforderliche Hard- und Software muss auf einem aktuellen Stand gehalten werden,
- alle notwendigen technischen, organisatorischen und personellen Rahmenbedingungen müssen geschaffen werden,
- alle relevanten Systeme müssen so konfiguriert werden, dass bekannte Möglichkeiten der Schwachstellenerkennung genutzt werden.

Anforderungen an die Protokollierung

Prinzipiell geht das BSI erst einmal davon aus, dass alle Basisanforderungen von OPS.1.1.5 erfüllt sein müssen. Darüber hinaus sieht es folgende Punkte als ein Muss an:

- Aufbau einer zentralen Protokollierungsinfrastruktur,
- Bereitstellung von Protokollierungsdaten für die Auswertung sowie
- Prüfung, ob alle geplanten Protokollierungsquellen gemäß Planung umgesetzt werden.

Muss-Anforderungen an die Detektion:

- alle Protokolldaten müssen kontinuierlich überwacht und ausgewertet werden,
- für die Detektion von sicherheitsrelevanten Ereignissen müssen genügend personelle Ressourcen bereitgestellt werden,
- Schadensdetektionssysteme müssen zentral verwaltet eingesetzt werden. Anhand des Netzplans muss festgelegt sein, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen,
- Übergänge zwischen internen und externen Netzen müssen um netzbasierte Intrusion Detection Systems (NIDS) ergänzt werden,
- eine zeitliche Synchronisation muss erfolgen,
- Ereignismeldungen müssen regelmäßig auf Auffälligkeiten kontrolliert werden,
- es muss eine Auswertung von Informationen aus externen Quellen erfolgen,
- die Auswertung der Protokolldaten muss durch spezialisiertes und qualifiziertes Personal erfolgen,
- zentrale softwaregestützte automatisierte Analysen mit Software müssen eingesetzt werden, um alle Protokollierungs-

ereignisse aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen,
- die Protokollierungsdaten müssen lückenlos einsehbar sein und permanent ausgewertet werden,
- werden definierte Schwellenwerte überschritten, muss automatisch alarmiert werden,
- die Systemverantwortlichen müssen die Analyseparameter regelmäßig auditieren und anpassen,
- bei einem sicherheitsrelevanten Ereignis müssen die eingesetzten Parameter das Ereignis automatisch melden und in Netzen, wo die kritische Dienstleistung nicht gefährdet ist, muss es möglich sein, automatisch mit geeigneten Schutzmaßnahmen zu reagieren,
- der Ausschluss von Netzen oder Netzsegmenten von einer automatischen Reaktion muss begründet sein.

Anforderungen an die Reaktion:
- festgestellte Sicherheitsvorfälle im vermeintlichen Zusammenhang mit Angriffen müssen gemeldet werden,
- Sicherheitsvorfälle, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit der kritischen Infrastruktur führen oder führen können, müssen an die zuständige Behörde gemeldet werden, entsprechend müssen auch Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen, gemeldet werden,
- die zur Angriffserkennung eingesetzten Systeme sollten automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbesdingten Störungen ergreifen können, wenn das zugrunde liegende sicherheitsrelevante Ereignis (SRE) eindeutig qualifizierbar ist. Dabei muss es gewährleistet sein, dass automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.

Beim letzten Punkt muss aus praktischer Sicht darauf verwiesen werden, dass der Begriff „eindeutige Qualifizierbarkeit eines sicherheitsrelevanten Ereignisses" unbedingt genauer zu definieren ist. In der Regel hinterlassen Cyber-Kriminelle weder eine Visitenkarte noch ein Manual.

Bewertung der Systeme zur Angriffserkennung

Die Systeme zur Angriffserkennung sollen nach folgenden „Reifegradmodell" bewertet werden. Die Stufen des Reifegradmodells sind wie folgt definiert:
- 0: Es sind bisher keine Anforderungen umgesetzt und es bestehen auch keine Planungen zur Umsetzung von Anforderungen.
- 1: Es bestehen Planungen zur Umsetzung von Anforderungen, jedoch für mindestens einen Bereich noch keine konkreten Umsetzungen.
- 2: In allen Bereichen wurde mit der Umsetzung von Anforderungen begonnen. Es sind noch nicht alle Muss-Anforderungen umgesetzt worden.
- 3: Alle Muss-Anforderungen wurden für alle Bereiche umgesetzt. Idealerweise wurden Sollte-Anforderungen hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.
- 4: Alle Muss-Anforderungen wurden für alle Bereiche umgesetzt. Alle Sollte-Anforderungen wurden umgesetzt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.
- 5: Alle Muss-Anforderungen wurden für alle Bereiche umgesetzt. Alle Sollte-Anforderungen und Kann-Anforderungen wurden für alle Bereiche umgesetzt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Für alle Bereiche wurden sinnvolle zusätzliche Maßnahmen entsprechend der Risikoanalyse/Schutzbedarfsfeststellung identifiziert und umgesetzt. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.

Nachweiserbringung

Zeitnah, das heißt vor dem 1. Mai 2023, wird das BSI ein entsprechendes Formular zur Verfügung stellen. Aller Voraussicht nach wird dieses in einer überarbeiteten Version der BSI-Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG zu finden sein.

Es ist davon auszugehen, dass ein Nachweis zu Angriffserkennungssystemen als vollständig erachtet werden wird, wenn die Ergebnisse der Prüfung der Systeme zur Angriffserkennung inklusive aufgedeckter Sicherheitsmängel inkludiert sind.

Fazit

Dass am 1. Mai 2023 Systeme zur Angriffserkennung implementiert sein müssen, ist allen Beteiligten bekannt. Bis dato gab es jedoch noch Interpretationsspielräume, welche Anforderungen die Systeme zur Angriffserkennung erfüllen müssen. Durch den BSI-Entwurf im Rahmen der Orientierungshilfe zum Einsatz von Systemen der Angriffserkennung wurde Klarheit geschaffen. Es ist zu erwarten, dass dieser Entwurf bald finalisiert wird. Und auch wenn er nicht finalisiert wird, so ist dies zur Pflicht der Umsetzung kein Problem, da die Orientierungshilfe nicht 1:1 umzusetzen ist.

Prof. h. c. PhDr. Stefan Loubichi

IT-/OT-Sicherheitsexperte mit dem Branchenschwerpunkt Energiewirtschaft, zuletzt unter anderem als leitender Auditor für ISMS-Systeme, Fachautor für VGB und Cyber-Security-Verantwortlicher für diverse Unternehmen.
stefan.loubichi@mailbox.org