Risiken für kritische Infrastrukturen

Automatische Bewertung auf Basis von CSAF

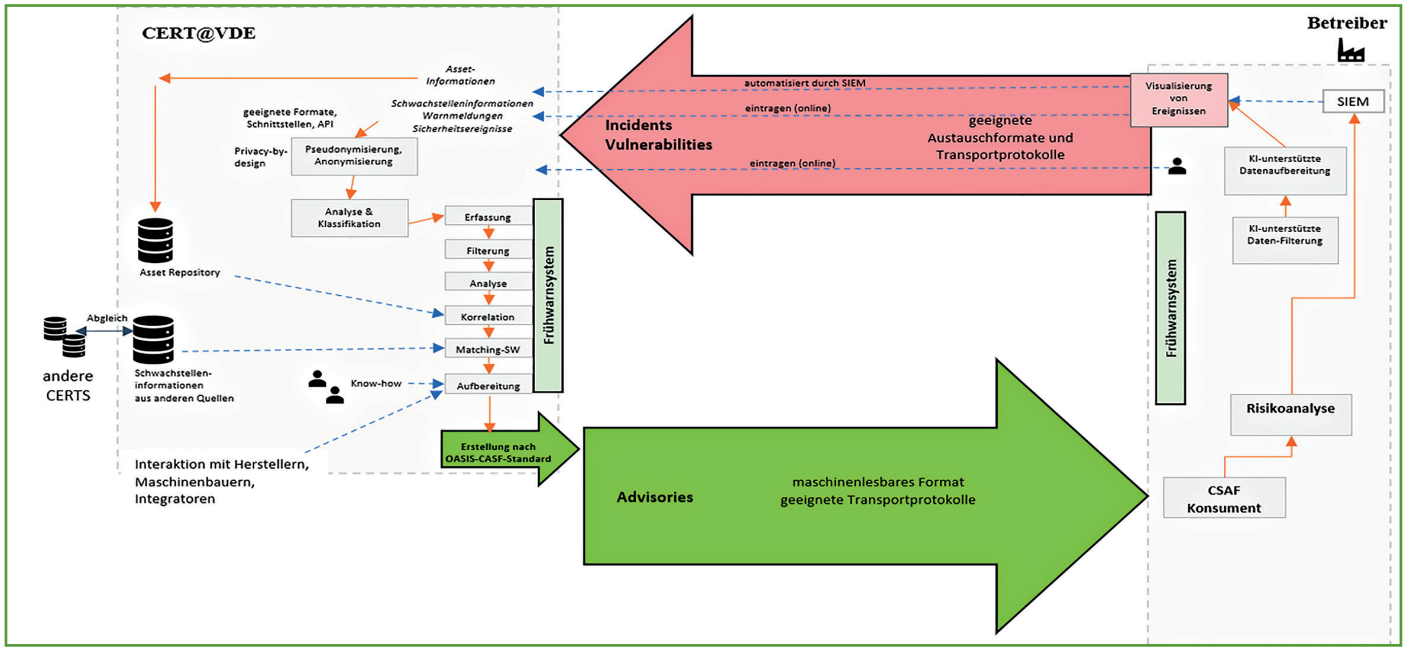

Abbildung 1: Architektur des ZenSIM4.0-Projektes. Im ZenSIM4.0-Projekt wurde ein CSAF-Demonstrator entwickelt, der die Kommunikation zwischen Betreiber und CERT automatisieren soll

Kai-Oliver Detken

Damit Unternehmen vor Software-Schwachstellen geschützt werden können, müssen kontinuierlich Updates installiert werden. Dabei kann die planlose Installation von Updates negative Folgen hinsichtlich der Verfügbarkeit haben und zu Ausfällen führen, weshalb eine Risikobetrachtung und -abwägung immer sinnvoll ist.

Prof. Dr.-Ing. Kai-Oliver Detken studierte Informationstechnik an der Universität Bremen und promovierte im Fachbereich Informatik. Heute ist er Geschäftsführer der DECOIT GmbH & Co. KG, doziert an der Hochschule Bremen und arbeitet als freier Autor im IT-Umfeld

Um diese durchführen zu können, müssen dem Unternehmen alle relevanten Informationen über neue Schwachstellen bereitgestellt werden. Dies geschieht aktuell durch sogenannte Security Advisories (SA), die menschenlesbare Informationen enthalten und von den Herstellern oder Koordinationsstellen veröffentlicht werden. Das neue Rahmenwerk Common Security Advisory Framework (CSAF) ermöglicht zum ersten Mal eine Automatisierung zum Auffinden, Bewerten und Umsetzen von SAs. Daher hat das BSI dessen Verbreitung ausdrücklich befürwortet.

Ausgangssituation

Unternehmen müssen zum Schutz ihrer Daten nicht nur ihre IT-Infrastruktur absichern, sondern auch die OT-Infrastruktur sowie ihre Produkte aus diesem Umfeld (Industrial Control Systems, ICS). Dieser Schutz muss der aktuellen Bedrohungslage Rechnung tragen.

Während große Unternehmen meist über ein eigenes CERT (Computer Emergency Response Team) verfügen und große Hersteller oft ein Product Security Incident Response Team (PSIRT) betreiben, besitzen klein- und mittelständische Unternehmen (KMU) kaum diese Ressourcen. Damit fehlt den KMUs auch die notwendige Vernetzung sowie der Austausch mit anderen CERTs. Darüber hinaus koordinieren sich CERTs untereinander (zum Beispiel bei der Bekämpfung von Bot-Netzen) und tauschen sicherheitsrelevante Informationen (zum Beispiel neue Schwachstellen bei OpenSSL) vertraulich und im Vorfeld öffentlicher Diskussionen untereinander aus. In Deutschland wird die übergeordnete CERT-Institution durch das BSI verkörpert.

Eine weitere Herausforderung im Bereich des Schwachstellenmanagements besteht darin, dass es kein einheitliches, maschinenlesbares „Advisory-Format“ gibt. Insbesondere fehlen spezifische Anforderungen der Maschinenbau- sowie der Automatisierungsindustrie. Derzeitige Aktivitäten bei der Organization for the Advancement of Structured Information Standards (OASIS) zur Standardisierung eines solchen Formats werden unter Beteiligung des deutschen CERT@VDE mit Anforderungen aus der hiesigen Automatisierungsindustrie unterstützt. Es sollen dadurch weitergehende Ansätze und Bedarfe für KMUs in einem Standard integriert und Anwendungshilfen (u. a. Tools zur Generierung, Bearbeitung und Verarbeitung von Warnmeldungen) zur Verfügung gestellt werden.

CSAF 2.0

Das Common Security Advisory Framework (CSAF) ist ein offener Standard, der das Schwachstellenmanagement verbessern soll, indem strukturierte, maschinenlesbare und interoperable Security Advisories (SA) zur Verfügung gestellt werden. Dadurch kann eine automatisierte Verarbeitung und die Integration in Sicherheitstools wie Schwachstellenmanagementsysteme oder Plattformen zur „Threat Intelligence“ erfolgen. CSAF in der Version 2.0 wurde von der OASIS Open-Organisation entwickelt und ist seit 2022 ein offizieller Standard. CSAF 2.0 standardisiert die Beschreibung und den Austausch von Schwachstellen-Informationen im JSON-Format, um:

- Automatisierung zu ermöglichen
- Interoperabilität zwischen Tools und Organisationen sicherzustellen
- Transparenz und Verlässlichkeit von SAs zu erhöhen

Durch eine maschinelle Verarbeitung kann die Verarbeitungsgeschwindigkeit und damit die Reaktionszeit deutlich gesteigert werden. Ebenso schnell und automatisiert sollten Betroffene reagieren können, um potenzielle Gefahren abzuwehren. Die meisten Technologie-Anbieter veröffentlichen sogenannten „Good Practice Guides“, nach deren Vorgaben Kunden und Anwender die Hard- oder Software des Anbieters möglichst sicher konfigurieren und nutzen können. Informationen über Schwachstellen in Hard- und Software ihrer Produkte werden von den meisten Herstellern zudem in sogenannten Security Advisories zur Verfügung gestellt. Darin enthalten sind Kennungen resp. Identifikatoren (IDs), um die Schwachstelle eindeutig zu bestimmen. Eine solche Kennung ist die Common Vulnerabilities and Exposures ID (CVEID). Weiterhin enthalten sind Informationen zum Hersteller, eine Liste betroffener Produkte, eine Einschätzung der Gefährdungslage und empfohlene Gegenmaßnahmen. Die Kritikalität der Schwachstelle wird dabei meist durch den einheitlich verwendeten „CVSS Base Score“ dargestellt. Zur Abwehr und Abschwächung der Risiken werden als Gegenmaßnahmen meist Patches und Software-Updates veröffentlicht oder Konfigurationsänderungen empfohlen. Diese Aktualisierungen und Änderungen sollten bei einer tatsächlich existenten Bedrohung möglichst zeitnah umgesetzt werden, um Schwachstellen zu schließen, bevor sie ausgenutzt werden können, was durch den CSAF-Ansatz ermöglicht wird.

Forschungsprojekt ZenSIM 4.0

Im Rahmen des Forschungsprojekts ZenSIM 4.0 wurde eine für mittelständische Unternehmen im Industrie4.0-Bereich spezifische Demonstrator-Plattform entwickelt (siehe Abbildung 1), die den unterstützten Einstieg in ein hochqualitatives Incident-Management vermitteln sollte. Mittels der Plattform können Unternehmen nun Informationen zu ihrer IT- und OT-Infrastruktur und ihren schützenswerten Assets, ihren bereits verwendeten Sicherheitsmaßnahmen sowie in der Vergangenheit ereigneten Sicherheitsvorfällen bereitstellen. Im Sinne des Crowd-Sourcings können so verteilte Erfahrungen und Informationen von einer Vielzahl von KMUs auf der gesicherten Plattform datenschutz-gerecht gesammelt und aufbereitet werden. Als Gegenleistung für die Teilnahme und die Preisgabe ihres Wissens können KMUs wirtschaftlich fundierte Sicherheitsempfehlungen zum Beispiel zu Exploits und Schwachstellen spezifisch für ihre IT-Infrastruktur und Assets erhalten. Zudem wurde im Demonstrator eine Vielzahl von Schwachstelleninformationen aus verschiedenen Quellen in die Plattform eingespeist, sodass ein KMU beispielsweise die Risikolage einschätzen kann, um geeignete Maßnahmen einleiten zu können. KMUs können so für sich fachlich relevante Warnungen individuell auswählen und konsumieren (Warenkorbansatz), ohne dass hierfür ein eigenes CERT aufgebaut werden muss. Ohne eine Versorgung mit entsprechenden Warnungen und Meldungen bleiben KMUs der Automatisierungsindustrie ohne diese überaus wichtige Unterstützung und ohne Zugang zu kritischen Informationen, obwohl sie selbst kritische Anlagen entwickeln, aufbauen, steuern und betreiben. Dies gefährdet nicht nur die Zukunftsfähigkeit der Betriebe, sondern auch sehr direkt die Betreiber und betroffene Anwender beziehungsweise Bürger durch angreifbare Systeme und Anlagen, wenn Sicherheitslücken weder geschlossen noch Angriffe erkannt beziehungsweise kommuniziert werden.

CSAF-Demonstrator

Im ZenSIM4.0-Projekt wurde daher ein CSAF-Demonstrator entwickelt, der die Kommunikation zwischen Betreiber und CERT automatisieren soll. Der in Abbildung 1 als roter Pfeil bezeichnete Prozess beschreibt die Kommunikation zwischen dem Betreiber und dem CERT@VDE,

der Partner in diesem Projekt war. In diesem Prozess meldet der Betreiber einen Vorfall an das CERT@VDE und soll dazu möglichst viele relevante Informationen übermitteln, damit über das CERT der entsprechende Hersteller alarmiert werden kann. Für den Fall, dass bereits ein Patch verfügbar ist, kann der Betreiber direkt wichtige Hilfestellungen und Informationen über den grünen Pfeil erhalten, um die Schwachstelle bei sich schließen zu können. Handelt es sich um eine bisher unbekannte Schwachstelle, wird der Hersteller beginnen, einen entsprechenden Patch zu entwickeln, der später auch die Betreiber erreichen wird.

Dieser in Abbildung 1 als grüner Pfeil benannte Prozess kann und sollte automatisiert werden und bezieht sich dann auf die Kommunikation zwischen einem CSAF-Aggregator und einem CSAF-Consumer. Der CSAF-Aggregator stellt beim CERT gesammelte und eventuell aufbereitete Schwachstelleninformationen in Form von CSAF-Dokumenten zur Verfügung, die vom CSAF-Consumer heruntergeladen und verarbeitet werden. Die automatisierte Verarbeitung von CSAF-Dokumenten umfasst neben der Kommunikation vom CSAF-Aggregator zum CSAF-Consumer auch die Verarbeitung der CSAF-Dokumente bis hin zur Ticketerstellung in einem System zur Angriffserkennung (SzA), was durch ein Security Information and Event Management (SIEM) realisiert werden kann.

Abbildung 2 zeigt mit dem SIEM-System ScanBox, wie eine mögliche CSAF-Integration aussehen könnte, die im Projekt exemplarisch umgesetzt wurde . Der CSAF-Aggregator stellt dabei die zentrale Anlaufstelle von CSAF-Dokumenten dar, die über den Update-Service in der CSAF-Datenbank abgelegt werden. Die Datenbank befindet sich im Netz des Betreibers und kann für weitere Analysen genutzt werden. Die Asset-Datenbank enthält schützenswerte Komponenten (Server, Laptops, Netzwerkgeräte etc.), die vom SIEM-System gesammelt

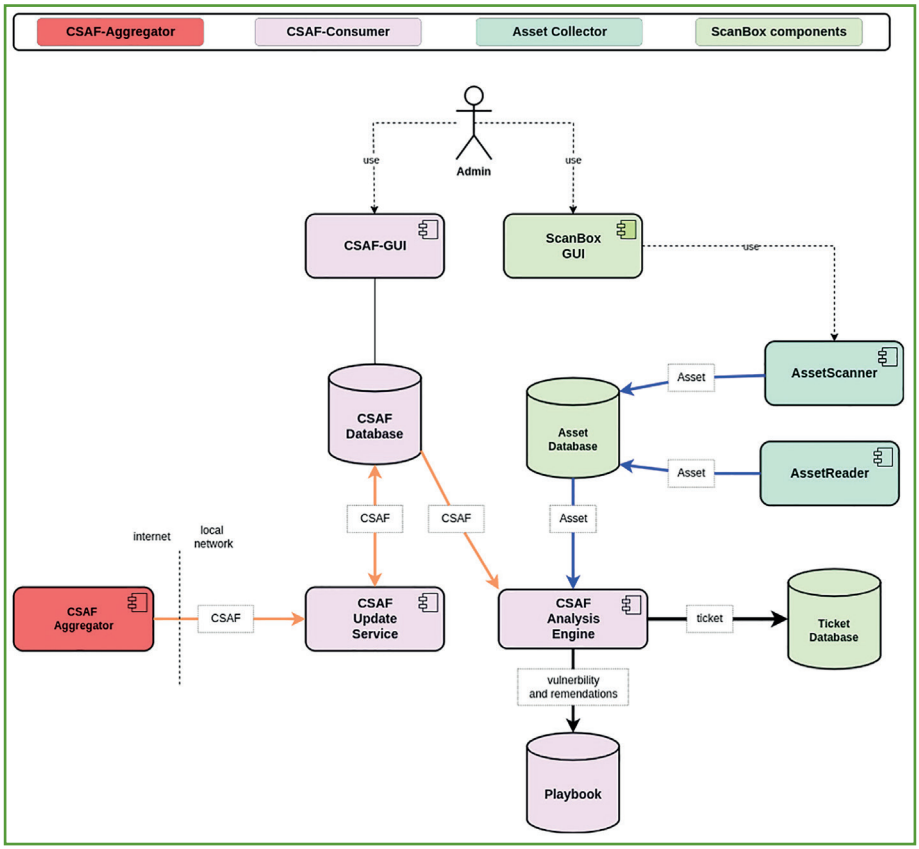

Abbildung 2: SIEM-Architektur mit CSAF-Verbraucherkomponente. Der CSAF-Aggregator stellt dabei die zentrale Anlaufstelle von CSAF-Dokumenten dar, die über den Update-Service in der CSAF-Datenbank abgelegt werden (Grafiken: Detken)

und überwacht werden. In regelmäßigen Abständen wird nach neuen Assets im Netzwerk gesucht, da man bei einer Sicherheitsanalyse alle Komponenten kennen muss. Die Playbook-Datenbank enthält Empfehlungen zur Behebung von Schwachstellen. Sie sind mit CVEs und den entsprechenden Assets verknüpft.

Der CSAF-Update-Service ist ein Teil des CSAF-Consumers. Die Hauptaufgabe dieser Komponente ist es, die lokale CSAF-Datenbank auf der Seite des Betreibers aktuell zu halten. In der CSAF-Analyse-Engine verbirgt sich der CSAF-Asset-Matcher, der CSAF-Dokumente mit Assets assoziiert. Trifft die Beschreibung eines CSAF auf ein Asset zu, wird ein CSAF-Asset-Match erzeugt. Wenn dies geschieht, wird ein Ticket für das SIEM-System ScanBox erzeugt. Die eindeutige Identifizierung von Assets ist dabei von entscheidender Bedeutung für das Matching gegen CSAF-Advisorys. In der CSAF-Spezifikation wurden daher Felder definiert, die zur korrekten Identifizierung von Assets verwendet werden können. Aufgrund der Tatsache, dass eine eindeutige Identifikation eines Assets nur innerhalb eines Namensraumes möglich ist, ist es notwendig, den entsprechenden Namensraum eines Assets zu bestimmen.

Fazit

CSAF 2.0 ist ein entscheidender Baustein für die Automatisierung und Standardisierung von Security Advisorys. Es ermöglicht eine schnellere, genauere und sicherere Reaktion auf Schwachstellen. Daher fördert das BSI eine Verbreitung dieses Standards. Alleine durch das kommende NIS2-Sicherheitsgesetz werden zirka 38.000 Unternehmen dazukommen, die gesetzlich Sicherheitsvorfälle an das BSI schicken müssen. Und diese Informationsflut kann nur durch eine entsprechende Automatisierung gehandhabt werden. Der CSAF-Demonstrator des ZenSIM4.0-Projekts hat gezeigt, dass dies möglich ist.