Technische und organisatorische Maßnahmen nötig

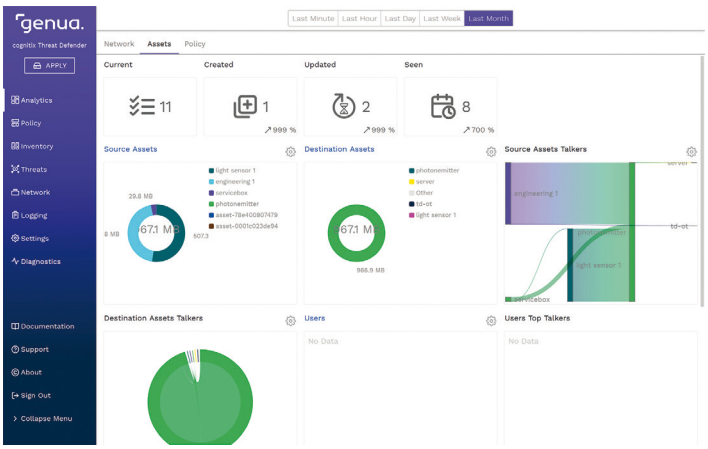
Worauf es bei der Erkennung von Angriffen ankommt

Im September letzten Jahres hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) seine Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung final veröffentlicht – und damit die Anforderungen aus dem IT-Sicherheitsgesetz 2.0 weiter konkretisiert. Eine wichtige Rolle spielen dabei die Aufgaben Protokollierung, Detektion und Reaktion. Worauf es dabei ankommt und wie KRITIS-Betreiber eine passende Lösung noch termingerecht umsetzen können, erklärt dieser Beitrag.

Von Arnold Krille, genua GmbH

Paragraf 8a des BSI-Gesetzes (BSIG) verpflichtet Betreiber kritischer Infrastrukturen ab dem 1. Mai 2023 Systeme zur Angriffserkennung (SzA) einzusetzen. Diese gelten als effektive Maßnahme, um Cyberangriffe frühzeitig zu erkennen und Schäden zu vermeiden oder zumindest zu vermindern. Um für betroffene Unternehmen bei der individuellen Umsetzung der neuen gesetzlichen Anforderungen zusätzliche Klarheit und Sicherheit zu schaffen, hat das BSI Ende September 2022 eine „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ herausgegeben. Sie soll künftig auch prüfenden Stellen als Anhaltspunkt dienen.

Gemäß Orientierungshilfe lassen sich die technischen Funktionen und Aufgabenbereiche von Systemen zur Angriffserkennung drei Bereichen zuordnen: Protokollierung, Detektion und Reaktion. So müssen die Systeme durch fortlaufende Auswertung der gesammelten Informationen sicherheitsrelevante Ereignisse erkennen, beispielsweise durch Missbrauchs- oder Anomalie-Erkennung. Betreiber sollten ferner Maßnahmen implementieren, um Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren. Das kann sowohl durch technische als auch durch organisatorische Maßnahmen umgesetzt werden.



Der cognitix Threat Defender zeigt aufsummiert, welche Assets in den letzten 30 Tagen wie viel Datenverkehr initiiert beziehungsweise beantwortet haben sowie den Datenverkehr zwischen den Assets. Die Qualität von Angriffserkennung ist davon abhängig, dass Assets und Kommunikation im Netzwerk vollständig gescannt werden können.

Protokollierung in der Angriffserkennung

In der gängigen IT-Infrastruktur haben sich zentrale Protokollierungsdienste und Log-Management-Lösungen weitgehend etabliert. Sie ermöglichen eine umfassende Analyse von Vorgängen und Angriffen. Anders sieht es dagegen im Internet der Dinge aus, beispielsweise bei vernetzten Maschinen und Anlagen in der industriellen Produktion. Ein zentrales Logging ist hier bisher nur sehr selten anzutreffen, jedoch unerlässlich, um Störungen und Angriffe effektiv zu erkennen und zu bekämpfen. Eine zentrale Erfassung der relevanten Logdaten aller Komponenten ist darum Pflicht.

Auch gibt es Komponenten im Netz, die aufgrund ihrer beschränkten Ressourcen neben der normalen Funktion keine zusätzlichen Logging-Aufgaben übernehmen können. In solchen Fällen ist eine Überwachung des entsprechenden Netzwerksegments von außen notwendig. Auch diese Überwachungserkenntnisse müssen in das zentrale Logging eingespeist werden.

Die Qualität der Erkennung ist davon abhängig, dass ein System zur Angriffserkennung ein Netzwerk vollständig scannen kann. Relevante Daten sind beispiels-

weise, welche Geräte im Netzwerk vorhanden sind, wer mit wem kommuniziert, und welche Kommunikationsprotokolle wie häufig verwendet werden. Daher empfiehlt das BSI, zusätzlich ein System zur Netzwerküberwachung zu installieren, selbst wenn alle Geräte ihre Aktivitäten eigenständig protokollieren können. Denn nur mit einer breiten Datenbasis kann die nachfolgende Detektion erfolgreich sein.

Auffälligkeiten analysieren und richtig bewerten

Die durch die Protokollierung erzeugten Daten müssen auf Abweichungen analysiert werden. Dabei ist es nicht ratsam, sich allein auf eine technische und automatische Analyse zu verlassen. Stattdessen muss zwingend ein Mensch die Protokolle regelmäßig und vollständig auf Auffälligkeiten prüfen.

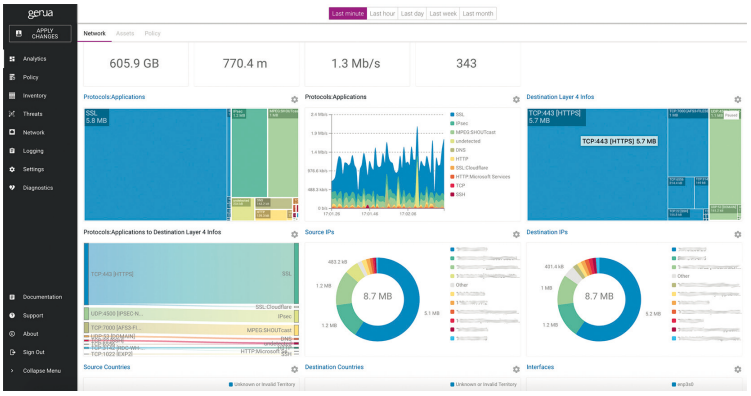
Das BSI ist sich der Schwierigkeit bewusst, dass technische Systeme zwar sehr gut Abweichungen von gelernten Mustern erkennen, jedoch nur sehr schlecht deren Auswirkungen einschätzen können. Zumal in gängigen Anlagen (gewollte) Änderungen die Lernfähigkeit von automatischen Methoden regelmäßig überfordern. Das Erkennen von neuen und unbekannten Störungen und die Bewertung, ob es sich um Störfälle, Probleme oder gar Angriffe handelt, obliegt also explizit dem Fachpersonal.

Effektive Reaktion braucht ein klares Lagebild

Auf die mit der Detektion erkannten sicherheitsrelevanten Ereignisse muss dann adäquat reagiert werden. Neben der Benennung von Verantwortlichen sind hier vor allem die Definition und Einhaltung von standardisierten Vorgehensweisen wichtig. Nur wenn alle Beteiligten und Betroffenen schnell ein klares Bild von der Bedrohung und der nötigen Reaktion haben, kann auch effektiv reagiert werden.

Dabei ist es elementar wichtig, zwischen mehr oder weniger drastischen Maßnahmen der Angriffsbekämpfung auf der einen und der Sicherstellung der eigentlichen Kernaufgabe der kritischen Infrastruktur auf der anderen Seite abzuwägen. Auch die passende und zeitnahe Information an die jeweils relevanten Meldestellen muss definiert sein.

Je schneller und umfassender Maßnahmen erfolgen, umso effektiver wirken sie. Daher wird zumindest in weniger kritischen Bereichen auch die automatische Reaktion nicht nur empfohlen, sondern muss möglich sein. Die Überwachung eines Netzwerkes mit der Möglichkeit des aktiven und automatisierten Eingreifens muss also von Anfang an berücksichtigt werden.



Blick ins Cockpit des cognitix Threat Defender. Nur wenn alle Beteiligten und Betroffenen schnell ein klares Bild von der Bedrohung und der nötigen Reaktion haben, kann effektiv reagiert werden.

Angriffserkennung mittels Anomalieerkennung

Wie sich Protokollierung, Detektion und Reaktion mit Anomalieerkennung nach aktuellem Stand der Technik unterstützen lassen, sei am Beispiel des cognitix Threat Defender (genua GmbH) erklärt. Die Lösung erfüllt alle wesentlichen gesetzlichen Anforderungen an ein technisches System zur Angriffserkennung. cognitix Threat Defender zeichnet sich unter anderem durch eine sehr gute Erkennung von Netzwerkkomponenten aus und bezieht alle maßgeblichen Systeme, Komponenten oder Prozesse wie IT, OT, Rechenzentren und Embedded-Systeme ein. Betreiber können relevante Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Werden Auffälligkeiten entdeckt, steht ein abgestuftes Spektrum an Reaktionsmöglichkeiten zur Verfügung. Neben der Meldung von Anomalien können Geräte und Kommunikation beispielsweise isoliert, verlangsamt oder vollständig blockiert werden. Um bei unklarer Bedrohungslage unnötige Beeinträchtigungen im Netzwerk zu vermeiden, kann cognitix Threat Defender im Fall einer Inzidenz auch adaptiv reagieren. Dann lässt er für das betroffene Gerät im Netzwerk nur jene Aktionen zu, die in den vergangenen 24 Stunden als „normal“ gelernt wurden. Alles, was davon abweicht, wird gedrosselt oder blockiert und an die Security-Verantwortlichen gemeldet. Damit gewinnen diese Zeit für eine angepasste und effektive Reaktion.

Organisatorische Maßnahmen unterstützen

Ein System zur Abwehrerkennung beschränkt sich laut BSI allerdings nicht allein auf technische Lösungen, sondern umfasst auch organisatorische Maßnahmen, um die Cybersicherheit eines Unternehmens sicherzustellen. cognitix Threat Defender als technische Komponente ist darum auch mit Blick auf die Usability entwickelt worden. Mit der modernen Benutzeroberfläche werden dem Verantwortlichen die relevanten Informationen auf einfache Weise dargestellt und geben damit schnell die „situational awareness“.