Sicherheitsempfehlung

Anomalieerkennung in kritischen Infrastrukturen

Martin Ortgies

Für die Erhöhung der Sicherheit kritischer Infrastrukturen (Kritis) gibt es neue Anforderungen, auf die sich Betreiber einstellen sollten: eine hochproblematische Cyberbedrohungslage, die Cybersicherheitsempfehlung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) „Monitoring und Anomalieerkennung" sowie die verpflichtende Vorgabe einer „Angriffserkennung" im Entwurf zum IT-Sicherheitsgesetz 2.0. Das Thema Angriffs- bzw. Anomalieerkennung steht also auf der Tagesordnung. Zu Recht.

Martin Ortgies, freier Journalist in Hannover, im Auftrag von Corning Services

Im Zeitraum 2018/2019 hat das BSI rund 114 Mio. neue Schadprogrammvarianten und bis zu 110.000 Bot-Infektionen täglich in deutschen Systemen registriert", so das BSI im aktuellen Bericht „Die Lage der IT-Sicherheit in Deutschland 2019". Dabei hat das BSI wiederholt auf die gestiegene Gefahr von Ransomware-Angriffen (wie durch Emotet) mit Produktionsausfällen, Schäden in Krankenhäusern und kommunalen Einrichtungen hingewiesen. Laut einer aktuellen Studie des Bitkom ist der Schaden durch digitale Angriffe fast doppelt so hoch wie noch vor zwei Jahren.

Neue Anforderungen für Kritis-Betreiber

Weil die Komplexität der Netze und die IT-Sicherheitsrisiken steigen, nennt das BSI in einer Cybersicherheitsempfehlung „Monitoring und Anomalieerkennung" als notwendig zur Prävention, Detektion und Reaktion und „zur Erkennung solcher Angriffe mehr denn je erforderlich."
Die Cybersicherheitsempfehlung des BSI:

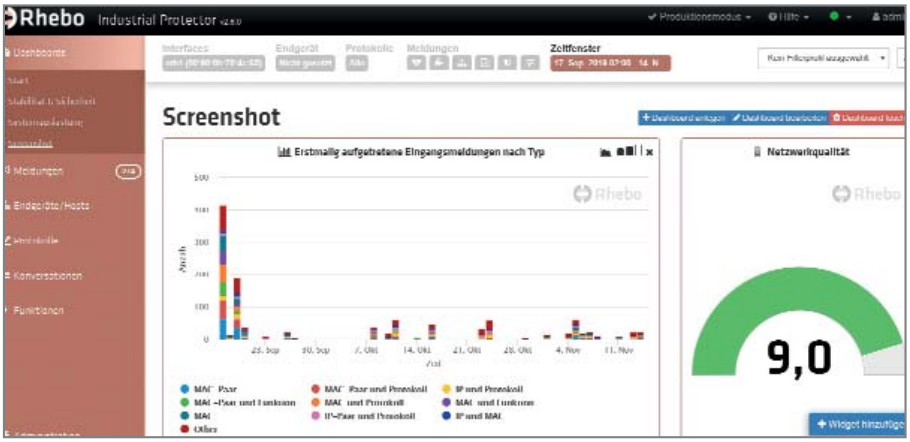
- Monitoring dient zum kontinuierlichen Überwachen von Prozessen, Geräten, Kommunikationsbeziehungen und Diensten innerhalb eines Netzes. Dazu gehört auch das Auslösen von Meldungen und Alarmen bei Erkennen besonderer Ereignisse.
- Anomalieerkennung ist ein Mittel zum Schutz von Netzen aller Art. Sie ermöglicht die Erkennung untypischen Verhaltens und somit neben technischen Fehlerzuständen und Fehlkonfigurationen auch die Detektion bisher unbekannter Angriffsformen auf solche Netze. Dies unterscheidet die Anomalieerkennung von anderen Maßnahmen, die auf der Erkennung bereits bekannter Angriffe beruhen. (BSI-CS 134 vom 25. Februar 2019)

Neue Anforderungen durch IT-SiG 2.0

Der Entwurf zum „IT-Sicherheitsgesetz 2.0" (IT-SiG 2.0) bringt für die Betreiber kritischer Infrastrukturen zusätzliche Anforderungen. Dazu gehört auch der verpflichtende Einsatz von Systemen zur „Angriffserkennung". „Diese Systeme stellen eine effektive Maßnahme zur Begegnung von Cyber-Angriffen dar." (IT-SiG 2.0 vom 27. März 2019).
Laut BSI gehört die Anomalieerkennung zu den grundsätzlichen Methoden der Angriffserkennung (Intrusion Detection). Anomalien, also Abweichungen von „normalen Betriebszuständen", treten meist in einem Fehlerfall auf. Sie können allerdings auch ein Hinweis auf einen Angriff bzw. eine Manipulation innerhalb eines Netzes sein, so das Bundesamt.

Lösung für die Anomalieerkennung

Corning Services hat mit dem Technologieunternehmen Rhebo einen Partner gefunden, der bei Lösungen für die Anomalieerkennung (Anomaly Detection) führend ist. Der Rhebo Industrial Protector ist in der Lage, in vernetzten Produktionsanlagen und in kritischen Infrastrukturen bisher nicht oder erst sehr spät entdeckte Angriffe auf Kommunikationsnetze frühzeitig zu erkennen. Dazu überwacht die Software an neuralgischen Punkten des Netzes den Datenverkehr in Echtzeit. Hierbei werden die Daten ohne Rückwirkungen auf die Prozesse im Netz rein passiv erfasst. Die Lösung erkennt ungewöhnliches Verhalten im Netzverkehr, das vom Normalzustand abweicht. Dazu setzt die Angriffserkennung auf eine intelligente Auswertung des Datenstroms durch Deep Packet Inspection und maschinelles Lernen. Darüber hinaus erkennt die



Die Anomalieerkennung erkennt untypisches Verhalten und neben technischen Fehlerzuständen und Fehlkonfigurationen auch die Detektion bisher unbekannter Angriffsformen

Lösung auch Fehler und Mängel im Netz.

Ausgangspunkt der Anomalieerkennung ist ein Stabilitäts- und Sicherheitsaudit des Netzverkehrs. Dafür werden die selbstlernenden Algorithmen in einer ein- bis zweiwöchigen Lernphase mit dem normalen täglichen Kommunikationsverhalten der Geräte und Anwender im Netz intensiv trainiert. Dieses Audit bietet zudem eine schnelle und vollständige Risikoanalyse der eingesetzten Geräte, Systeme, Verbindungen und Kommunikationsmuster. Das Ergebnis ist ein Security-Report. Er schlägt operative Maßnahmen vor, um erkannte Strukturschwächen in den Netzen zu beseitigen. Denn festgestellte Anomalien können sowohl durch eine Malware oder Cyberattacken verursacht werden als auch durch fehlerhafte Datenpakete, Netzprobleme, Kapazitätsengpässe oder Anpassungen im Netz. So greift die Software auch auf das Verzeichnis der Common Vulnerabilities and Exposures (CVE) mit bekannten Sicherheitslücken in Netzgeräten zu. Außerdem werden operative Mängel im Netz gelistet, wie ungepatchte Systeme, unnötige Protokolle, fehlerhafte Gerätekonfigurationen, unerwünschte Aufrufe von IP-Adressen oder ungeplanter Traffic. Diese Mängel zeigen Schwachstellen auf, die von Angreifern genutzt werden können.

Nach Abschluss der Einführungsphase werden Abweichungen im Datenverkehr als Anomalien gemeldet. Das Betriebspersonal wird durch Schulungen auf die Bearbeitung solcher Meldungen gut vorbereitet. Zugang zu den erfassten Daten haben ausschließlich Mitarbeiter mit besonderen Nutzerrechten. Die Daten sind auch vom Hersteller der Software nicht einsehbar. Bei Bedarf steht Corning Services als Servicepartner auf Abruf, um Meldungen des Systems zu analysieren.

Wenn interne Ressourcen fehlen

Häufig ist fehlendes Personal eine große Hürde für den Einsatz der Anomalieerkennung. Hier übernimmt beispielsweise das Network Operating Center (NOC) von Corning Services weitergehende Security-Dienstleistungen wie die zeitweise oder kontinuierliche 24/7-Überwachung der Anomaliedetektion. Das NOC übernimmt das Monitoring, untersucht und bewertet

Wenn beim Betreiber die Ressourcen fehlen, übernimmt das Network Operating Center (NOC) von Corning Services die zeitweise oder kontinuierliche 24/7-Überwachung der Anomaliedetektion (Bilder: Corning Services)

die Meldungen und informiert den Betreiber unmittelbar über sicherheitsrelevante Vorkommnisse. Zusätzlich erfolgen ein wöchentlicher Report und eine monatliche Besprechung der Ergebnisse. *(bk)*