Ziel: Resilienz

Anomalieerkennung für kritische Infrastrukturen

Martin Ortgies

Bei der Sicherheit kritischer Infrastrukturen (Kritis) gibt es Handlungsbedarf. Herkömmliche Schutzmechanismen reichen nicht mehr aus, weil die wechselseitigen Abhängigkeiten vernetzter Systeme steigen und sich die Zahl und Professionalität der Angriffe weiter erhöhen. Das Konzept der Anomalieerkennung verspricht einen zusätzlichen Schutz für Kommunikationsnetze. Eine Analyse.

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

Die im Jahr 2018 bekanntgewordenen Zugriffe auf Büronetze in der Energiebranche offenbaren laut Bundesamt für Sicherheit in der Informationstechnik (BSI), dass es womöglich nur eine Frage der Zeit ist, bis kritische Systeme erfolgreich angegriffen werden können. Der BSI spricht von einer neuen Qualität der Gefährdung. Bisherige Abwehrmaßnahmen verlieren demnach weiter an Wirksamkeit.

Es können nicht alle Angriffe verhindert werden

Ausgereifte Schutzsysteme wie Firewalls, Virenscanner, Intrusion-Detection-Systeme, Datenverschlüsselungen oder Maßnahmen zur Netzsegmentierung sorgen für ein hohes Sicherheitsniveau. Mit Einführung des Informationssicherheitsmanagementsystems (ISMS) nach ISO/IEC 27001 und 27019 werden die technischen Maßnahmen und organisatorischen Verfahren in einen dauerhaften Prozess eingebunden. Die zunehmende Komplexität durch die Energiewende, die Ausweitung der Energiewende auf die Sektoren Wärme und Verkehr und die Digitalisierung stellen die Stabilität und Sicherheit des Energiesystems allerdings grundlegend infrage. Aktuelle Ansätze der Cybersicherheit gehen davon aus, dass es trotz der Sicherheitsmaßnahmen auf Dauer nicht möglich sein wird, alle Angriffe zu verhindern.

Die Schlussfolgerung: Die Netze müssen „resilient" werden, also bei Störungen ihre grundlegende Funktionsfähigkeit erhalten oder zumindest eigenständig wiedererlangen können, wie es z.B. in der Analyse „Ausfallsicherheit des Energieversorgungssystems – Von der Robustheit zur Resilienz" des Bitkom steht. Das Resilienzkonzept geht davon aus, dass die hundertprozentige Absicherung jedes angeschlossenen Gerätes und jeder Anlage nicht möglich ist. Demnach muss das System als Ganzes über wirksame Erkennungs- und Abschottungsmechanismen für Angriffe und Ausfälle verfügen. Mithilfe von Informations- und Kommunikationstechniken können Störungen frühzeitig erkannt, Gegenmaßnahmen eingeleitet und Systemdienstleistungen übernommen werden. „So bietet z.B. die automatische Erkennung von Anomalien in Netzdaten mithilfe des maschinellen Lernens neue Möglichkeiten der Gefahrenabwehr im Cyberraum", heißt es.

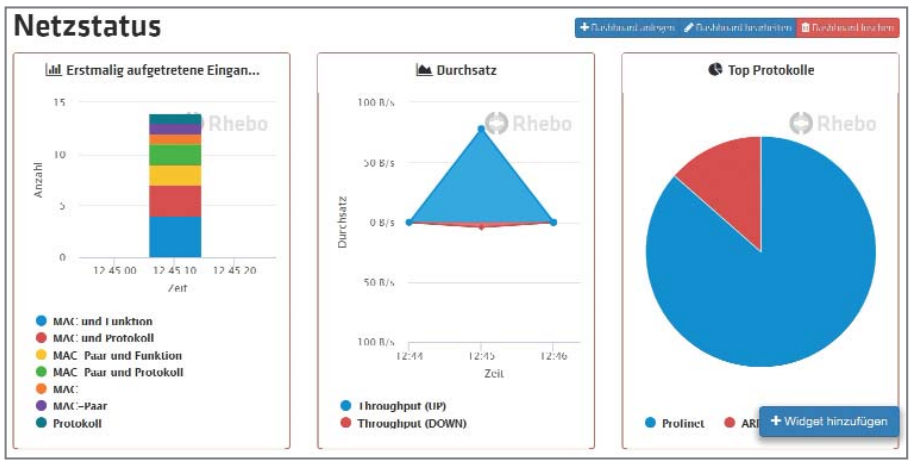
Die Besonderheiten kritischer Infrastrukturen

Die Analyse des Bitkom folgert, dass durch eine permanente Analyse der Datenströme in Echtzeit entstehende Störungen im Energiesystem frühzeitig erkannt werden können. So lasse sich über die Identifikation verräterischer oder normabweichender Muster Störungen erkennen, während sie sich noch anbahnen. „Dies ermöglicht es, proaktiv zu reagieren, d.h. die Störungen zu antizipieren und sie durch geeignete Gegenmaßnahmen zu verhindern oder zumindest so klein wie möglich zu halten", so der Bitkom.

Strategien zur Cybersicherheit in kritischen Infrastrukturen wie Fernwirknetzen unterscheiden sich grundlegend von IT-Netzen in Büroumgebungen. Kritis-Netze sind stärker abgeschirmt, unterliegen einer geringeren Dynamik durch neue Anwendungen, Geräte oder Netzanpassungen und verwenden sehr spezifische Steuerungsprotokolle wie IEC 60870-5-104.

Systeme zur Anomalieerkennung (Anomaly Detection) können in kritischen Infrastrukturen zuverlässig eingesetzt werden, wenn sie auf die Besonderheiten dieses Umfelds eingestellt werden (*Bild*). Hier setzt das Konzept von Corning Services (die frühere 3M Services) an. Zum Portfolio des Systemintegrators gehören Security-Lösungen

wie Anti Fraud, Anti DDoS, Verschlüsselungen auf allen Netz-Layern, Secure-Gateways zum Absichern von Fernwirkstationen und auch die Anomalieerkennung. Corning Services unterstützt die Betreiber von Netzinfrastrukturen zudem durch Managed Services bis hin zur Betriebsführung und ist außerdem Teilnehmer der BSI-Allianz für Cybersicherheit. Auf diesem Erfahrungshintergrund basiert die Auswahl einer Lösung für die Anomalieerkennung von Rhebo, das sich auf die Ausfallsicherheit industrieller Steuerungssysteme mittels Überwachung der Datenkommunikation spezialisiert.



Systeme zur Anomalieerkennung können in kritischen Infrastrukturen zuverlässig eingesetzt werden, wenn sie auf die Besonderheiten dieses Umfelds eingestellt sind

Wie eine Software für die Anomalieerkennung arbeitet

Die Softwarelösung zur Anomalieerkennung ist darauf ausgerichtet, bisher nicht oder erst sehr spät erkannte Angriffe auf Kommunikationsnetze frühzeitig zu detektieren. Dazu überwacht sie an neuralgischen Punkten des Netzes den Datenverkehr in Echtzeit. Hierbei werden die Daten ohne Rückwirkungen auf die Prozesse im Netz rein passiv erfasst.

Um ein ungewöhnliches Verhalten im Netzverkehr zu erkennen, das vom Normalzustand abweicht, setzt die Software auf eine intelligente Auswertung des Datenstroms durch Deep Packet Inspection und maschinelles Lernen. Damit die Anomalieerkennung nicht auf das Erkennen bereits bekannter Gefahren beschränkt bleibt, werden die selbstlernenden Algorithmen in einer mehrwöchigen Lernphase mit dem normalen täglichen Kommunikationsverhalten der Geräte und Anwender im Netz intensiv trainiert.

Der Einführungsprozess für eine Netzinfrastruktur beginnt mit der Installation der Datensensoren und der Anomalieerkennungssoftware im Lernmodus. Nach einer ca. zweiwöchigen Lernphase erfolgt ein Workshop zur Bewertung der Netzkommunikation, in der die Erfahrungen und das Know-how der Administratoren und Netztechniker eine wichtige Rolle spielen. Sie können beurteilen, welche Form der Kommunikation und Konnektivität für das Netz gewünscht und normal ist. Gemeinsam werden alle Meldungen der Software ausgewertet und die erwünschten Aktivitäten im Netz auf einer Whitelist gespeichert. Dabei können die Meldungen durch Filtermechanismen zusammengefasst werden. Anschließend ist das System betriebsbereit.

Nach der Lernphase erstellt Corning Services mit den Ergebnissen der Software einen Security-Report. Er basiert auf einer professionellen Analyse des Netzes und 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 Computersystemen zu. So werden u.a. Geräte erkannt, die noch mit alten Firmwarebeständen arbeiten. Auf diese Weise können auch operative Mängel im Netz erkannt werden, wie die Verwendung für das Netz unnötiger Protokolle, fehlerhafte Gerätekonfigurationen, unerwünschte Aufrufe von IP-Adressen oder ggf. nicht beantwortete Anfragen von Fernwirkgeräten. Diese Mängel zeigen Schwachstellen auf, die von Angreifern genutzt werden können. Durch ihre Beseitigung kann die Stabilität und Sicherheit der Netze weiter erhöht werden. Mithilfe der Analyse des Netzverkehrs lassen sich aus der Anomalieerkennung auch einfach erweiterte Filterregeln für Firewalls ableiten, die die Netzsegmentierung erhöhen und damit Angriffsszenarien für Cyberattacken minimieren.

Serviceunterstützung für den Betrieb

Nach Abschluss der Einführungsphase werden Abweichungen im Datenverkehr als Anomalien gemeldet. Diese können verursacht werden durch neue Teilnehmer im Netz, neue Kommunikationsbeziehungen zwischen den Teilnehmern, den Einsatz bisher nicht verwendeter Protokolle, durch neue Operationen mit einem bekannten Protokoll oder durch abweichende Antwortzeiten bei bekannten Operationen. Für forensische Analysen speichert die Software die Kommunikationsdaten vor und nach dem Auftreten der Anomalie. Das Betriebspersonal wird durch Schulungen auf die Bearbeitung solcher Meldungen gut vorbereitet. Corning Services steht zusätzlich als Servicepartner auf Abruf, um Meldungen des Systems zu analysieren. Zudem übernimmt das NOC von Corning Services weitergehende Security-Dienstleistungen wie die zeitweise oder kontinuierliche 24/7-Überwachung der Anomaliedetektion.

Die Daten der Anomalieerkennung können außerdem dem Security Information and Event Management (SIEM) übergeben werden. Die Software unterstützt auch die Zertifizierung nach 27001 sowie die Meldepflicht bei Vorfällen gemäß IT-Sicherheitsgesetz. *(bk)*