genua.

Ein neuer Ansatz für die IT-Sicherheit in Produktionsnetzen

Für die IT-Sicherheit in Produktionsnetzen besteht dringender Handlungsbedarf, denn die weitere Vernetzung von Maschinen und Anlagen durch Industrie 4.0 und IoT erhöht die Sicherheitsrisiken beträchtlich. Cyberattacken auf die Informationstechnik in Produktionsumgebungen (Operational Technology, OT) sind häufig erfolgreich, weil die vorhandenen IT-Securitylösungen keinen ausreichenden Schutz bieten. Dieses Whitepaper erläutert, wie mit der neuen Sicherheitslösung, dem cognitix Threat Defender, die Sicherheit in OT-Netzen erhöht werden kann.

SecurITy made in Germany

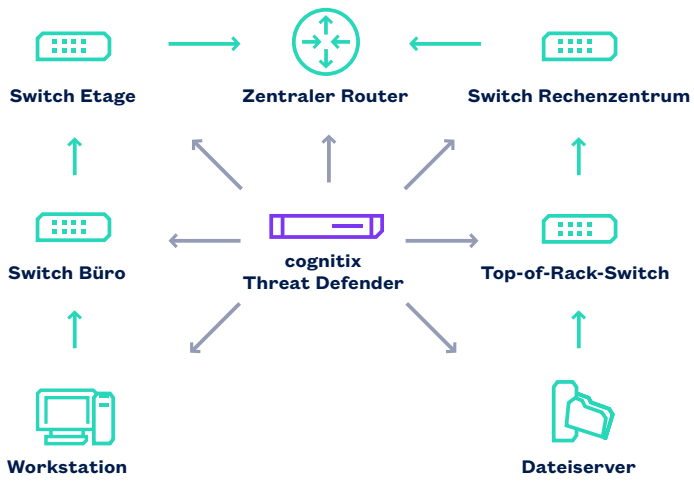
Inhalt.

1. Aktuelle Bedrohungen für Produktionsnetze

Mit Industrie 4.0 werden Produktionsnetze und Services „smart“ – indem Maschinen und Anlagen, industrielle Steuerungssysteme (Industrial Control Systems, ICS) sowie Automationslösungen online vernetzt und Produktionsnetze flexibler und effizienter gemacht werden. Für den Datentransfer oder für Fernwartungszugriffe wird die bisherige physische Trennung der OT von anderen IT-Systemen und Office-Netzen aufgehoben. OT-Netze, Logistikprozesse oder Systeme der Gebäudeleittechnik werden dadurch anfälliger für Angriffe von außen.

Die Herausforderung: Klassische IT-Sicherheitskonzepte sind für OT-Netze meistens nicht anwendbar. Viele Systeme laufen auf veralteten Betriebssystemen. Sicherheitsupdates oder nachträgliche Härtungsmaßnahmen können häufig nicht umgesetzt werden. Höchste Verfügbarkeits- und Integritätsanforderungen lassen Eingriffe in laufende Systeme oftmals nicht zu. Zudem haben die Anlagen mit Lebenszyklen von 30 und mehr Jahren meist ein geringes Sicherheitsniveau. Risiken entstehen aber nicht nur durch die Onlineverbindungen. Durch infizierte USB-Sticks, mobile Endgeräte wie dem Laptop des Servicetechnikers oder durch eine fehlende Segmentierung des OT-Netzes werden auch offline betriebene Anlagen durch Schadprogramme infiziert.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor einer hohen Dynamik bei der Weiterentwicklung von Schadprogrammen und Angriffswegen. Annähernd 70 Prozent der Unternehmen und Institutionen in Deutschland sind demnach bereits Opfer von Cyber-Angriffen geworden. Dabei bleiben erfolgreiche Cyber-Attacken häufig unentdeckt. Die Angriffe werden verschleiert, Manipulationen sind unauffällig und die Veränderungen oft schleichend. Die Folgen sind dennoch drastisch. Durch die Manipulationen werden Anlagen zerstört und sensible Safety-Systeme ausgeschaltet. Bereits jeder zweite erfolgreiche Angriff führte in der Vergangenheit zu Produktions- bzw. Betriebsausfällen, so das BSI.



Der innovative cognitix Threat Defender geht über Intrusion Prevention hinaus: Mit KI-, Data Analytics- und Threat Intelligence-Funktionen baut er eine zweite Verteidigungslinie im Netzwerk auf und ergänzt damit die Firewall-Lösungen, die den Datenverkehr an den Schnittstellen kontrollieren und sichern.

2. Wie können OT-Netze geschützt werden?

Ein wirksamer Schutz für die Vertraulichkeit, Integrität und Verfügbarkeit von OT-Netzen ergibt sich aus dem Zusammenspiel von Regeln, Verfahren, Maßnahmen und Tools, wie sie u. a. im Informations-Sicherheits-Management-System (ISMS gemäß ISO/IEC 27000) und der Norm für „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“ (IEC 62443) definiert sind.

2.1 Defense-in-Depth-Prinzip (IEC 62443)

So ist in der Norm IEC 62443 ein Defense-in-Depth-Prinzip („gestaffelte Verteidigung“) verankert. Es definiert den Schutz gegen Cyberangriffe (wie bei einer Zwiebel) in mehreren Schichten. Auch wenn eine Sicherheitsschicht überwunden wurde, ist nur ein Teil des Netzes betroffen. Das Gesamtsystem ist noch durch weitere Sicherheitsebenen geschützt. So ist es sinnvoll, die Netzbereiche in unterschiedliche Sicherheitszonen aufzuteilen und gestaffelte Schutzlevel zu vergeben.

2.2 Sicherheitszonen, Zonenübergänge und Schutzlevel

Eine notwendige Maßnahme ist daher, unterschiedliche Sicherheitszonen festzulegen und voneinander abzuschotten. Die Zonenübergänge und die Kommunikation zwischen den Zonen können durch Firewalls und entsprechende Filterregeln restriktiv geregelt werden. So lassen sich auch abgesicherte Schleusen-PCs einrichten, um beispielsweise USB-Sticks verwenden zu können.

Für Zonen mit besonders hohem Schutzlevel können Datendioden eingesetzt werden. Eine Datendiode lässt ausschließlich einen Einbahn-Datentransfer zu. In der Gegenrichtung wird der Informationsfluss abgeblockt. Geschützt hinter dieser Datendiode können Maschinen, Anlagen und IT-Systeme somit Daten von der Anlage zum Leitstand oder über öffentliche Netze zum Servicecenter des Herstellers versenden, ohne dass ihre Integrität gefährdet wird.

2.3 Absicherung der Fernwartung

Sichere Fernwartungs-Lösungen erlauben den Zugang nur zu einer Sicherheitszone. Dies kann mit einem sogenannten Rendezvous-Server umgesetzt werden, der in der demilitarisierten Zone (DMZ) neben der Firewall installiert wird. Durch diese neutrale Zwischenebene wird eine direkte Verbindung mit dem Internet ausgeschlossen. Hierhin bauen sowohl der Wartungs-Service als auch der Maschinenbetreiber zum vereinbarten Zeitpunkt verschlüsselte Verbindungen auf. Erst mit deren Rendezvous auf dem Server in der DMZ entsteht die durchgängige Wartungsverbindung zur betreuten Maschine.

2.4 Monitoring der Netzkommunikation (IDS/IPS)

Durch die immer ausgefeilteren Angriffszenarien und Angriffstechniken werden Cyber-Attacken immer effektiver im Datenstrom von z. B. HTTP, HTTPS, POP3 oder IMAP verschleiert. Die Kommunikation ist größtenteils verschlüsselt und schwer zu überprüfen. Ein Angriff und die Aktivität von Malware sind deshalb oft nicht auf den ersten Blick zu erkennen. So finden Schadprogramme trotz Firewall und Virenscanner einen Weg in das OT-Netz.

Das Monitoring von OT-Netzen ist hier eine zusätzliche Schutzmaßnahme, um die Anlagenkommunikation zu überwachen und auf Auffälligkeiten zu untersuchen. Dafür haben sich Intrusion-Detection-Systeme (IDS) und Intrusion-Prevention-Systeme (IPS) etabliert. Sie werden bereits seit vielen Jahren in Office-Netzen eingesetzt.

IDS-Systeme analysieren den Datenstrom im OT-Netz und alarmieren den Administrator bei einem verdächtigen Verhalten. Das IDS sucht dabei nach Mustern im Datenstrom einer Kommunikationsverbindung. Eine mögliche Schadsoftware wird mit Hilfe von Signaturen erkannt, die allerdings kontinuierlich aktualisiert werden müssen, um auch neue Schadvarianten entdecken zu können.

IPS-Systeme analysieren den Datenstrom und schützen zusätzlich vor einem Angriff, indem sie bei einem auffälligen Verhalten die Kommunikation sofort unterbrechen. IPS-Systeme konnten sich in OT-Netzen allerdings nicht durchsetzen. Sie haben ein relativ hohes Störungsrisiko, wenn die Signaturen beispielsweise zu Fehlalarmen (False Positive) führen und das IPS-System dann die Anlagenkommunikation unterbricht. Was bei Officenetzen ggf. toleriert werden kann, ist bei OT-Anlagen dagegen inakzeptabel.

2.5 Neue Anforderungen an die Sicherheitstechnik

Die Cyber-Sicherheits-Empfehlung des BSI (BSI-CS 134) hebt die Anomalieerkennung als ein Mittel zum Schutz von Netzwerken besonders hervor: „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.“

Die Forderung nach einer Anomalieerkennung findet sich auch im Entwurf „IT-Sicherheitsgesetz 2.0“ (IT-SiG 2.0). Die Betreiber kritischer Infrastrukturen werden demnach erstmals zum Einsatz von Systemen zur „Angriffserkennung“ verpflichtet. „Diese Systeme stellen eine effektive Maßnahme zur Begegnung von Cyber-Angriffen dar.“ (IT-SiG 2.0 vom 27.03.2019)

3. Sicherheitslücken in OT-Netzen

Ein wesentlicher Nachteil von IDS- und IPS-Systemen ist, dass sie auf Auffälligkeiten im Datenstrom begrenzt sind. Schickt beispielsweise eine beliebige Netzkomponente einen Steuerungsbefehl an eine Zentrifuge, ist im Datenstrom selbst nichts auffälliges und wird deshalb nicht detektiert. Das IDS-System überprüft nicht, ob diese Netzkomponente berechtigt ist, ein solches Signal zu senden. Es überprüft auch nicht, ob dieses Verhalten für diese Netzkomponente ungewöhnlich ist. So können Angreifer Geräte und Anlagenkomponenten im Netz übernehmen, ohne dass dies sofort auffällt.

4. Verhalten der Netzwerkkomponenten überwachen

Der cognitix Threat Defender schließt die Sicherheitslücke von IDS- und IPS-Systemen. Er überwacht den gesamten Netzwerkverkehr und analysiert auch das Verhalten der Netzkomponenten (Assets). Der cognitix Threat Defender richtet ein überwachtes sicheres Netzwerk ein, in dem er Verhaltensmuster der Netzwerkgeräte erkennt und definierten Regeln zuordnet. Dabei werden bisher getrennte Funktionen wie Netzwerkanalyse, Intrusion Detection, Asset Tracking und eine dynamische Policy Engine in einem System zusammengeführt.

4.1 Passives Monitoring

Der cognitix Threat Defender unterstützt ein passives Monitoring der Netzkommunikation, um OT-Netze nicht zu stören. Der Datenstrom wird überwacht und analysiert. Dabei liegt der Fokus nicht auf einem einzelnen Gerät oder einer einzelnen Netzverbindung, sondern auf der Kommunikation im gesamten Netzwerk und dem Verhalten aller Netzwerkteilnehmer.

4.2 Asset Tracking mit Realtime-Analyse

Durch ein Asset Tracking mit Realtime-Analyse wird eine Asset-Datenbank aller Geräte im Netzwerk angelegt und ein Netzwerkstatus im „Grundzustand“ erstellt. Es wird ermittelt, welche Devices sich im Netzwerk befinden und welcher Netzwerkverkehr in diesem Grundzustand stattfindet. Dazu wird der Netzwerkverkehr erfasst. Mit einer solchen Anfangsbestandsaufnahme des Netzwerks werden auch generelle Schwachstellen und Sicherheitslücken erkannt, die beispielsweise durch Konfigurationsfehler, Netzwerkprobleme, unbekannte oder nicht zugelassene Netzwerkelemente, bewusstes oder unbewusstes Fehlverhalten, sonstige „schwarze Flecken“ bis hin zu Angriffen im Netzwerk verursacht werden.

4.3 Threat Intelligence Datenbank

Der cognitix Threat Defender nutzt zusätzlich die internationale MISP-Datenbank für den automatisierten Austausch von Bedrohungsinformationen (Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing). In der Datenbank werden technische und nichttechnische Informationen zu Malware-Beispielen, Vorfällen, Angreifern, gefährlichen Websites, bekannten Command and Control Server (C&C) und weiteren Informationen gespeichert. MISP wird weltweit von mehr als 6000 Organisationen genutzt. Diese Informationen werden im cognitix Threat Defender als zusätzlicher Kontext herangezogen und helfen bei der Beurteilung des Risikos im Netzwerk.

4.4 Automatisierte Anomalieerkennung

Der cognitix Threat Defender analysiert den Netzverkehr nach IP- und MAC-Adressen, Ports, Protokollen und Anwendungen der OSI-Schichten 2 bis 7. Dabei wird der Traffic auf problematische Adressen, Domains oder Dateisignaturen überprüft. Zusätzlich werden auf Basis der Asset-Datenbank die Kommunikationsbeziehungen der Geräte untersucht. Den Geräten werden Verhaltensregeln zugeordnet und diese überwacht.

Mit der automatischen Detektion des Netzwerktraffics werden ungewöhnliche und vom üblichen Standardverhalten abweichende Muster (Anomalien) im Datenstrom erkannt und so können Angriffe auf die Sicherheit frühzeitig abgewehrt werden.

Beispiele für Anomalien im Netzwerk
Eine Arbeitsstation, die bisher nur Verbindungen mit dem Anmelde- und File-Server hatte, kommuniziert plötzlich mit anderen Rechnern innerhalb des Netzwerks. So wird beispielsweise ein nicht erwünschtes File-Sharing der Arbeitsstation erkannt (Schatten-IT).

Bei der Überwachung wird ein physisches Gerät im Netzwerk erkannt, was nicht vorhanden sein sollte. Das kann z. B. ein Servicetechniker sein, der unerlaubt über Sicherheitszonen hinweg kommuniziert. Ein Drucker kontaktiert andere Geräte im Netz und will Code aus dem Netz nachladen, was auf eine Schadsoftware hindeutet.

Auch andere Beispiele passen zum Verhalten von Malware, wenn eine Workstation in kurzer Zeit Verbindungen zu vielen Ports aufnimmt (Netzwerkscan) oder wenn sich eine Pumpensteuerung plötzlich wie ein Human Machine Interface (HMI) verhält und Steuersignale an andere Komponenten der Anlage versendet.

Ein solches verändertes Kommunikationsverhalten von Netzkomponenten wird weder durch eine Firewall noch von einem IDS-System erkannt. Hier schließt der cognitix Threat Defender eine Sicherheitslücke.

4.5 Echtzeitreporting mit Alarmmeldungen

Der cognitix Threat Defender stellt dem Administrator ein Echtzeitreporting mit einem Ampelsystem zur Verfügung. Es liefert Meldungen über mögliche Gefahren und Angriffe. Dabei kann der Admin einstellen, ab welchem Level von Alarmmeldungen er informiert werden will. Es sind vier verschiedene Level verfügbar (1 High, 2 Medium, 3 Low, 4 Notice). Die Alarme können per E-Mail, Desktop Notification oder Web-Systemen versendet oder in ein bestehendes Alarmsystem (SIEM) integriert werden.

5. Best Practice: Anomalieerkennung in fünf Schritten

genua empfiehlt bei der Absicherung von gewachsenen OT-Netzen ein schrittweises Vorgehen. In der Praxis haben sich fünf Phasen bewährt.

5.1 Phase 1 – Assets katalogisieren

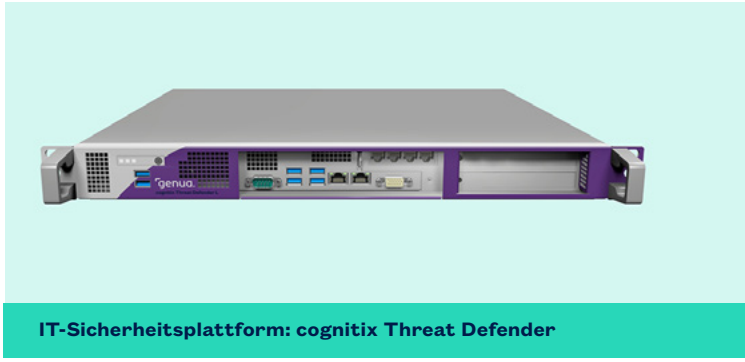
In der ersten Phase werden die Kommunikationspartner innerhalb des OT-Netzwerks ermittelt. Der Netzwerkverkehr wird im cognitix Threat Defender gespiegelt und alle aktiven Geräte im beobachteten Netzwerkbereich in einer Asset-Datenbank erfasst. Dabei werden für die Geräte Metadaten, wie zum Beispiel das verwendete Betriebssystem, identifiziert. Die Erfassung erfolgt rein passiv anhand des beobachteten Netzwerkverkehrs.

In dieser Phase werden bereits nach wenigen Stunden Fehlkonfigurationen, Netzwerkprobleme, veraltete Gerätesoftware oder nicht erlaubte Geräte erkannt. So fällt zum Beispiel eine fehlerhafte Konfiguration einer Active-Directory-Synchronisation auf. Diese kann einen konstanten Hintergrund-Traffic erzeugen, der zu keiner merklichen Einschränkung führt. Dennoch kann dieser Anzeichen eines Fehlers sein, weil die richtige Konfiguration eines AD nur bei Änderungen der Daten eine Synchronisation dieser Änderungen erfordert und damit wesentlich weniger Netzwerkverkehr erzeugt.

5.2 Phase 2 – Assets identifizieren

Im nächsten Schritt wird der Aufbau des Netzwerks untersucht, um bisher unbekannte Geräte im Netzwerk aufzuspüren und ggf. zu deaktivieren. So wird die Sicherheit erhöht und die Awareness für das Netzwerk verbessert.

Dazu wird die Asset-Datenbank manuell konsolidiert. Der Administrator des OT-Netzes ordnet die automatisch erfassten Assets einzelnen Geräten bzw. Geräteklassen zu. Dabei vergibt er aussagekräftige Namen und organisiert die Assets mittels Tags in domänenspezifischen Gruppen. Dieser manuelle Aufwand ermöglicht die Vereinfachung der Kommunikationsstrukturen und erleichtert die weitere Arbeit zur Analyse und Überwachung des Netzwerks.



IT-Sicherheitsplattform: cognitix Threat Defender

5.3 Phase 3 – Kommunikationspfade abbilden

Anschließend wird die Kommunikation der Geräte untereinander analysiert, um die zulässige Kommunikation in der Netzwerk-Policy zu modellieren. Unerwünschte Kommunikationspfade, nicht benötigte Dienste oder unerwünschte Protokolle, wie Multicast, werden deaktiviert.

Für diese zulässige Kommunikation werden nach und nach Regeln angelegt. Dies ist ein iterativer Prozess, bei dem immer wieder neue Tags und neue Regeln angelegt werden, bis eine feingranulare Netzwerk-Policy entsteht.

5.4 Phase 4 – Stabilisierung

Die erstellte Policy wird validiert und das Netzwerk passiv überwacht. Dazu läuft das erstellte Modell über mehrere Wochen passiv im OT-Netz. Der Administrator wird per E-Mail, Slack oder Syslog benachrichtigt, wenn die Logging-Regel greift und somit neue, noch nicht abgebildete Kommunikation erfasst wird. Gegebenenfalls muss die Policy dann nachjustiert werden. Wahrscheinlicher ist es jedoch, dass der neuartige Netzwerkverkehr eine Anomalie darstellt, die auf ein Problem oder gar eine Störung bzw. einen Eindringling hinweist.

5.5 Phase 5 – Aktives Blocking (optional)

Die ersten vier Phasen erfolgen lediglich an gespiegeltem Netzwerkverkehr, so dass für das OT-Netz keinerlei Risiko durch Latenzen oder Datenverlust besteht. Erst in der optionalen fünften Phase wird aktiv in den Netzwerkverkehr eingegriffen, um unerwünschte Kommunikation zu unterbinden. Dazu wird der Threat Defender vom Mirror-Port entfernt und direkt an den Netzwerk-Switch angeschlossen.

Für das aktive Blocking werden die in den Phasen 3 und 4 angelegten Regeln für die explizit erlaubte Kommunikation um Regeln ergänzt, die explizit verbotene und bei Bedarf auch jede unbekannte Kommunikation blockieren. Hierbei steigt mit der Sicherheit auch das Risiko für Unterbrechungen im OT-Netz, da nun keine unerwarteten Ereignisse mehr zulässig sind und von Threat Defender blockiert werden.

Um dieses Risiko zu reduzieren, ist es auch möglich, cognitix Threat Defender so einzurichten, dass er mit einem abgestuften Verhalten dynamisch auf Bedrohungen und Abweichungen reagiert („Adaptive Behavior-based Graylisting“). So wird der in Phase 3 und 4 festgelegte Netzwerkverkehr bedingungslos zugelassen. Neuer Verkehr wird zugelassen und für 24 Stunden als „bekannt“ gelernt. Wenn dann IDS, Threat Intelligence oder explizite Regeln für Verdachtsfälle ein Ereignis markieren, kann die als bekannt gelernte Netzwerkkommunikation weiterhin passieren. Die neue Kommunikation wird jedoch für ein paar Stunden unterbunden, eine Warnung ausgegeben und nicht als „bekannt“ angelernt. Wenn nun in diesem zweiten Abschnitt weitere Ereignisse auftreten oder der Administrator bei seiner Analyse ein Problem im Netzwerk bzw. in den Geräten erkennt, kann passend reagiert werden. Ansonsten wird nach dem Verstreichen der Zeit wieder in den normalen Modus zurückgeschaltet und neues Verhalten wieder als „bekannt“ gelernt. Damit kann auf neue und potenziell gefährliche Kommunikation reagiert werden, ohne die bestehende Kommunikation und damit die laufenden Prozesse zu behindern.

„Ein ganz wesentlicher Nutzen des cognitix Threat Defender ist der Gewinn an Transparenz des eigenen Netzwerks. Auf sichtbare Bedrohungen dann angemessen reagieren zu können, ist der große Bonus, wenn man den Überblick über das eigene Netzwerk gewonnen hat.“

Arnold Krille, Abteilungsleiter
Product Development cognitx Threat Defender

6. Zusammenfassung: Anomalieerkennung in einem OT-Netz

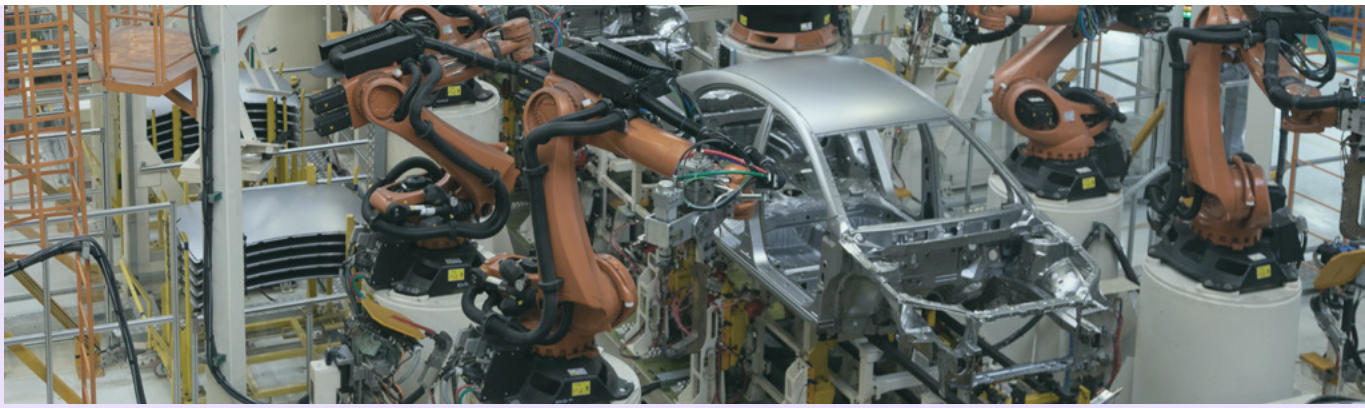
Mit Industrie 4.0 wird die bisherige physische Trennung der OT von anderen IT-Systemen und Office-Netzen aufgehoben. OT-Netze, Logistikprozesse oder Systeme der Gebäudeleittechnik werden dadurch anfälliger für Angriffe von außen. Gleichzeitig werden Cyber-Attacken durch die immer ausgefeilteren Angriffszenarien und Angriffstechniken immer effektiver und besser verschleiert. Schadprogramme finden deshalb trotz Firewall und Virenscanner einen Weg in das OT-Netz.

Ein wirksamer Schutz für die Vertraulichkeit, Integrität und Verfügbarkeit von OT-Netzen ergibt sich aus dem Zusammenspiel von Regeln, Verfahren, Maßnahmen und Tools (vgl. ISMS gemäß ISO/IEC 27000 bzw. IEC 62443). Die Cyber-Sicherheits-Empfehlung des BSI (BSI-CS 134) sowie der Entwurf „IT-Sicherheitsgesetz 2.0“ (IT-SiG 2.0) heben die Anomalieerkennung als ein Mittel zum Schutz von Netzwerken besonders hervor. Die dafür einsetzbaren Intrusion-Detection-Systeme (IDS) und Intrusion-Prevention-Systeme (IPS) sind allerdings auf die Erkennung von Auffälligkeiten im Datenstrom begrenzt. Die Systeme überprüfen nicht, ob eine Netzkomponente berechtigt ist, ein Signal zu senden. Sie überprüfen auch nicht, ob dieses Verhalten für diese Netzkomponente ungewöhnlich ist. So können Angreifer Geräte und Anlagenkomponenten im Netz übernehmen, ohne dass dies sofort auffällt.

Der cognitix Threat Defender schließt die Sicherheitslücke von IDS- und IPS-Systemen. Er überwacht den gesamten Netzwerkverkehr und analysiert auch das Verhalten der Netzkomponenten (Assets). Er richtet ein überwachtes sicheres Netzwerk ein, in dem er Verhaltensmuster der Netzwerkgeräte erkennt und definierten Regeln zuordnet. Er unterstützt ein passives Monitoring der Netzkommunikation, um OT-Netze nicht zu stören.

genua empfiehlt bei der Absicherung von gewachsenen OT-Netzen ein schrittweises Vorgehen. In der Praxis haben sich fünf Phasen bewährt (1 – Assets katalogisieren, 2 – Assets identifizieren, 3 – Kommunikationspfade abbilden, 4 – Stabilisierung und (optional) 5 – Aktives Blocking).

Der cognitix Threat Defender überwacht und analysiert den Datenstrom in einem automatisierten Prozess. Dabei liegt der Fokus nicht auf einem einzelnen Gerät oder einer einzelnen Netzverbindung, sondern auf der Kommunikation im gesamten Netzwerk und dem Verhalten aller Netzwerkteilnehmer. Die bisher getrennte Funktionen wie Netzwerkanalyse, Intrusion Detection, Asset Tracking und eine dynamische Policy Engine werden in einem System zusammengeführt.



Weitere Informationen:

www.genua.de/threat-defender

https://youtu.be/iHs62Xh68uM

Über genua

Die genua GmbH ist ein deutscher Spezialist für IT-Sicherheit. Seit der Firmengründung 1992 beschäftigen wir uns mit der Absicherung von Netzwerken und bieten hochwertige Lösungen. Unser Leistungsspektrum umfasst die Absicherung sensibler Schnittstellen im Behörden- und Industriebereich bis hin zur Vernetzung hochkritischer Infrastrukturen, die zuverlässigverschlüsselte Datenkommunikation via Internet, Fernwartungs-Systeme sowie Remote Access-Lösungen für mobile Mitarbeiter und Home Offices. Unsere Lösungen werden in Deutschland entwickelt und produziert. Viele Firmen und Behörden setzen auf Lösungen von genua zum Schutz ihrer IT. genua ist ein Unternehmen der Bundesdruckerei-Gruppe.

genua GmbH, Domagkstraße 7, 85551 Kirchheim bei München
T +49 89 991950-0, info@genua.de, www.genua.de