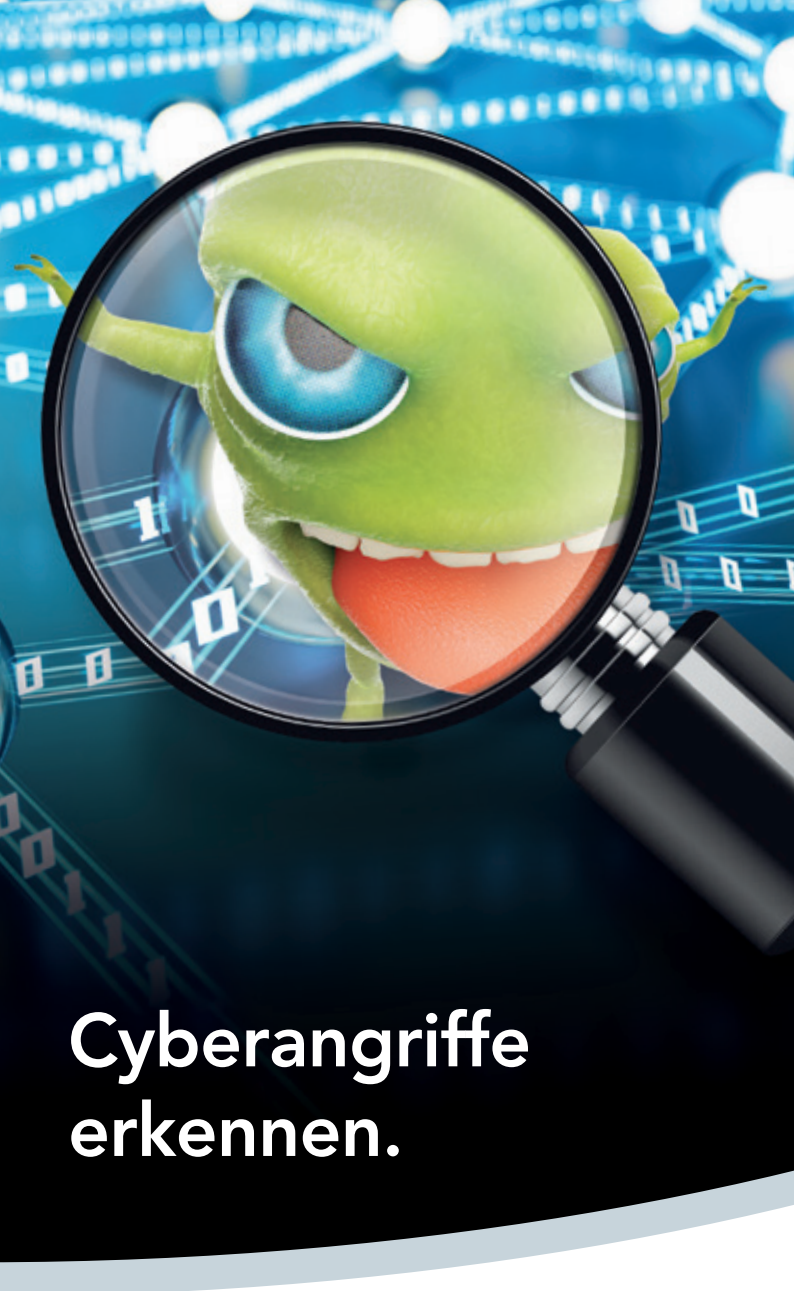


Cyberangriffe erkennen.

Rechtzeitig.

Mit Sicherheit verbunden.

mdex

Industrie 4.0:
Eine Firewall allein reicht nicht

Die Vernetzung von Produktionsanlagen eröffnet Industriebetrieben völlig neue Perspektiven. Mit Fernwartung und Früherkennung von Fehlern kann nicht nur die Produktionseffizienz signifikant erhöht werden. Die neue Qualität der Kommunikation macht etwa durch Production on Demand oder Pay per Use innovative Geschäftsmodelle überhaupt erst möglich. Doch spätestens seit dem Erpresser-Virus WannaCry ist klar, dass die Vernetzung der Industrieproduktion auch ein Einfallstor für Cyberkriminelle, Saboteure und Industrie-Spione ist.

Cyberattacken auf Industrieunternehmen sind längst kein abstraktes Risiko mehr: Im Mai 2017 hat beispielsweise der WannaCry-Virus mehr als 230.000 Computer in 150 Ländern infiziert. Europol sprach damals von einem noch nie dagewesenen Ereignis.

Ungebetene Gäste:
So tarnen sich Viren

Um eine Maschine oder Anlage zu infizieren, reicht ein USB-Stick, der Laptop eines Servicetechnikers oder auch ein erlaubter Fernzugriff. So verbreitet sich der WannaCry-Virus über eine Windows-Schwachstelle. Er verschlüsselt Daten auf dem befallenen System und fordert ein Lösegeld für die Entschlüsselung. Zuerst sucht der Virus aber gezielt nach weiteren Systemen im Netzwerk mit der gleichen Sicherheitslücke. Er will also zunächst unerkannt bleiben. Damit gibt es ein Zeitfenster, in dem ein befallenes System noch gerettet werden kann – falls der Angriff rechtzeitig erkannt wird.

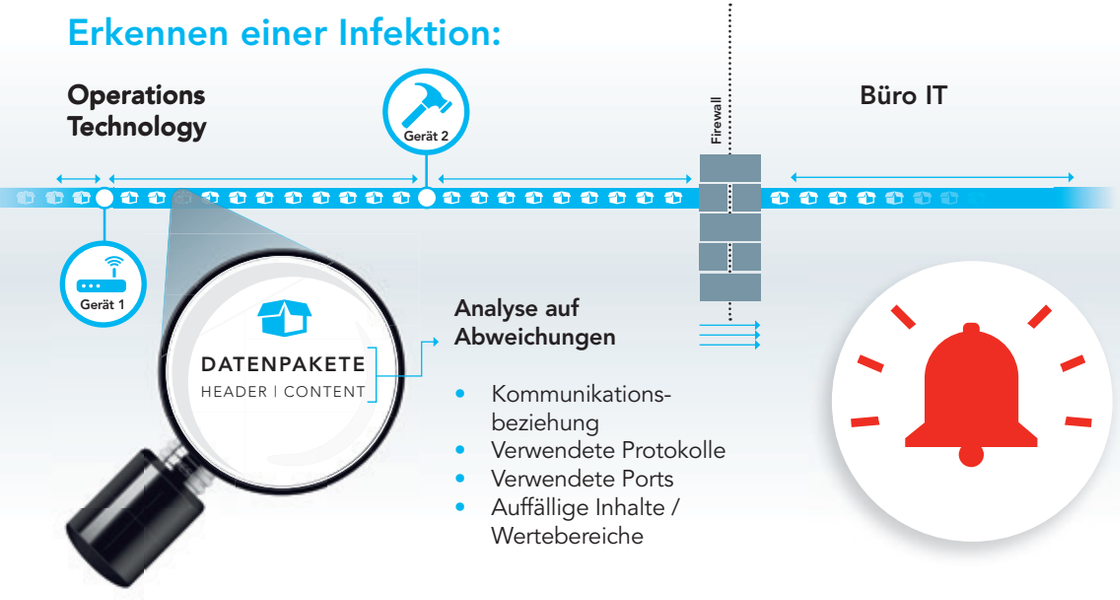
Frühwarnsystem durch
Deep Packet Inspection

Während dieser „Inkubationszeit" bauen Schadprogramme sehr viele neue Kommunikationsbeziehungen auf. Durch die Deep Packet Inspection werden diese bemerkt und ein Alarm ausgelöst. Im schlimmsten Fall muss nun lediglich der betroffene Industrie-PC neu aufgesetzt werden. Ein kostspieliger Produktionsausfall lässt sich noch verhindern. Das betrifft nicht nur Cyberangriffe: Sie sind stets über fehlerhafte Kommunikationsvorgänge informiert, um auf potentielle Störungen reagieren zu können, bevor die Gesamtanlage betroffen ist.

Individuelle Sicherheitslösungen mit mdex

Von mdex erhalten Sie nicht etwa ein Standard-Programm, sondern wir erarbeiten mit Ihnen ein maßgeschneidertes Sicherheits-Konzept. Zunächst gilt es, den Datenverkehr sinnvoll einzuschränken und zu kontrollieren. Eine Firewall sollte z. B. idealerweise nicht nur die internen IT-Systeme vom Internet trennen, sondern auch von den eigenen OT-Systemen (OT = Operational Technology) der Produktion. So kann im Detail geregelt werden, welche IT-Systeme mit welchen OT-Systemen überhaupt kommunizieren dürfen und welche Protokolle sie dafür verwenden.

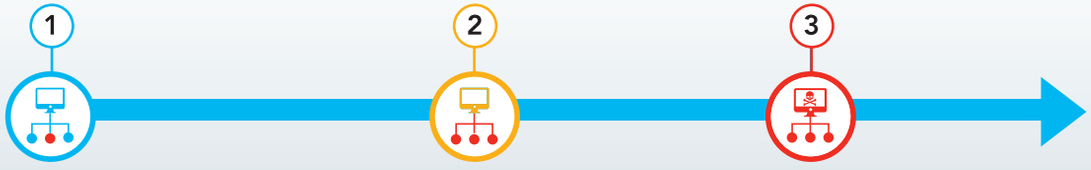
Erkennen einer Infektion:



mdex GmbH führt gemeinsam mit dem Kunden im Rahmen einer Deep Packet Inspection eine Analyse durch. Auffällige Protokolle, Ports oder Wertebereiche signalisieren so frühzeitig Anomalien, bevor das Schadprogramm einen größeren Schaden anrichten kann.

Zeitlicher Ablauf:

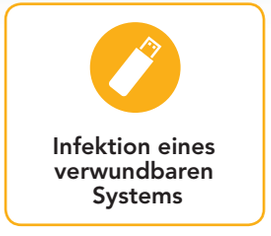
Viren werden z. B. über angeschlossene Hardware eingeschleust. Vorerst richtet das Programm häufig keine Schäden an, sondern infiziert zunächst unbemerkt das gesamte Netzwerk. Erst nach dieser Inkubationszeit legt die Malware das System lahm.



Infektion eines Systems z.B.
- mit einem USB-Stick
- angeschlossenes Service-Laptop etc.

System ist infiziert, jedoch weiter funktional. Aber:
- Aktive Infektion anderer Systeme über das Netzwerk

Alle verwundbaren Systeme sind infiziert und nicht funktional
- System ist kompromittiert/ funktionsunfähig



Ihr direkter Draht
zu den mdex Experts

Als ISO/IEC 27001 zertifizierter IT-Dienstleister hat mdex jahrelange Erfahrungen mit sicheren Kommunikationslösungen. Das mdex-Expertenteam berät Sie gern zu allen Themen der sicheren Kommunikation für technische Anlagen, sei es sichere Fernwartung, Predictive Maintenance, Stationsvernetzung oder eben auch zu Systemen zur Anomalie-Erkennung.

20 JAHRE
2017
mdex

Weitere Fragen?

Fon: +49 4109 - 555 444
Fax: +49 4109 - 555 101
Mail: frage@mdex.de