Netzwerk-Monitoring

„Noch werden viele Fehler gemacht"

Bild: Videc Data Engineering GmbH

Dieter Barelmann, Geschäftsführer der Videc Data Engineering GmbH

Um die Infrastruktur im eigenen Unternehmen vor Cyberangriffen schützen zu können, müssen Angreifer erst einmal entdeckt werden. Mit der Lösung IRMA will Videc Fertigungsbetrieben dabei helfen. Das System überwacht den Datenverkehr im Netzwerk, warnt vor unvalidierten Zugriffen und erlaubt eine Risikobewertung für unterschiedliche Unternehmens- und Anlagenbereiche. Dieter Barelmann, Geschäftsführer der Videc Data Engineering GmbH, spricht über die Herausforderung IT-Sicherheit und wie IRMA funktioniert.

ITP Wie verlaufen Angriffe auf Fertigungsnetzwerke typischerweise und wie sehen konventionelle Schutzmaßnahmen aus?
Dieter Barelmann: Ob speziell entwickelte Viren oder Bot-Netze – wir wissen natürlich nicht vorher, welche Angriffe stattfinden, aus welcher Richtung sie kommen und wer die Angreifer tatsächlich sind. Daher ist auch die Aufarbeitung von erfassten IT-Sicherheitsvorfällen so wichtig.

ITP Um das zu erleichtern, muss die Vorarbeit stimmen, oder?
Barelmann: Es gibt vom BSI viele Veröffentlichungen, wie Sie sich als Fertiger vor Angreifern schützen können, wie sich die Maßnahmen aufsetzen lassen und so weiter. Sie müssen die Sicherheit Ihrer Anlagen garantieren können, und das heißt für viele Unternehmen, das Thema auf der Agenda weiter nach oben zu setzen. Viele Unternehmen sind schon längst von Schadcode befallen, die noch nicht aktiv geworden sind, sondern die erst am Zeitpunkt X anfängt zu arbeiten.

ITP So wie Stuxnet in verschiedenen Anlagen weltweit gefunden wurde, ohne dort loszuschlagen?
Barelmann: Ja, genau. Schadsoftware ist ein Schwarzmarkt. Sie können im Internet schon Schadsoftware genau nach ihren Anforderungen bestellen. Es ist eine Illusion zu glauben, dass einem nichts passieren kann.

ITP Die Herausforderung IT-Sicherheit ist nicht neu. Ändert sich etwas mit der zunehmenden Vernetzung des Shop Floors?
Barelmann: Viele Unternehmen befassen sich gerade mit dem Thema IoT. Das bedeutet mitunter, dass sie irgendwie intelligente und quasi intelligente Geräte betreiben, die über das Internet kommunizieren. Sicherheitsmaßnahmen sind dabei oft vergessen worden. Gerade wenn offene Geräte verwendet wurden, ist in einigen Fällen im Prinzip ein Botnetz aufgebaut worden. Wenn dort eine Schadsoftware installiert wird, kann diese auf Befehl nach außen kommunizieren und sogar ganze Provider lahmlegen. Und wenn der Provider weg ist, können Sie erst einmal gar nichts dagegen machen.

ITP So wie beim groß angelegten Angriff auf einen DNS-Server in den USA Ende letzten Jahres. Die Dienste Twitter, Spotify, Airbnb, Reddit, Ebay und viele weitere waren über Tage kaum erreichbar.
Barelmann: Das sind Beispiele, wie Cyberangriffe funktionieren. Unter Umständen hätten auch die Dienste der Telekom tagelang ausfallen können. Wenn Sie eine Industrieanlage betreiben, müssen Sie sich genau überlegen, inwieweit Komponenten mit dem Internet verbunden sind. Sicherheitskonzepte müssen Fragen wie diese berücksichtigen und da werden meiner Meinung nach noch viele Fehler gemacht.

ITP Wie passt Ihr Ansatz IRMA – also 'Industrie Risiko Management Automatisierung' – ins Bild?
Barelmann: IRMA blockiert keine Angriffe oder Angriffsmechanismen. IRMA schützt den Scada-Bereich und die Automatisierung darunter, indem es das Netzwerk laufend überwacht und die Verbindung lässt sich Validieren. Das bedeutet, wenn Kommunikationspartner A mit B spricht, sieht das System die Kommunikation und ob sie in Ordnung ist oder nicht. Ändert sich das validierte Kommunikationsverhalten, wird eine Meldung generiert und an den Verantwortlichen weitergeleitet. Um das System einzurichten, sehen Sie sich erst einmal an, wer mit wem spricht und wer in welcher Art und Weise unerlaubt spricht und ob vielleicht noch Schnittstellen nach außen offen sind. Dabei scannt IRMA das gesamte Netzwerk passiv über den Mirrorport am managed Switch ab. Oft haben Integratoren irgendwann einmal einen Fernzugriff auf eine Anlage eingerichtet und nicht dokumentiert. So etwas erfahren Sie mit einer Monitoring-Lösung recht schnell. Auf dieser Basis lässt sich der Netzwerkverkehr bereinigen und diejenigen Verbindungen schließlich validieren, die erwünscht sind. Hat sich nun ein Unternehmen eine Schadsoftware eingefangen, wird diese immer versuchen, nach außen zu kommunizieren. Dazu werden auch interne Verbindungen benötigt. Diese nicht validierten Versuche, im Netzwerk zu kommunizieren, werden sofort erkannt. Anwender sehen, aus welchem Gerät diese Kommunikation stammt und können reagieren.

ITP Das Netzwerk-Monitoring muss in Prozesse eingebettet sein, es muss ein Alarmmanagement organisiert sein. Wie kompliziert ist es, das Werkzeug sinnvoll in einem Unternehmen aufzurollen?
Barelmann: Wir schließen das System an den Mirror Port eines intelligenten Switch an und schauen uns den Datenverkehr an, der über das Gerät geht. So können wir die Kommunikation beziehungsweise das Grundverhalten automatisiert einlesen. Sie parametrieren die Einheit anhand einer Beschreibung von vielleicht zwei Seiten. Dann ist IRMA mit dem Netzwerk verbunden, zeichnet die Kommunikation automatisch auf und ordnet sie IP-Adressen zu. Damit ergibt sich ein recht genaues Bild vom Datenaustausch im Betrieb. Bis dahin brauchen Sie nichts zu tun. Im nächsten Schritt können Sie die IP-Adressen in textliche Zusammenhänge bringen: SPS1, Rechner 1 oder Scada 1. Es muss einmal definiert werden, wer mit wem sprechen soll und wer nicht. Ab diesem Zeitpunkt zeigt das System valide und nicht valide Zugriffe an. Auf dieser Grundlage lassen sich Alarme einrichten.

ITP In IRMA steckt das Wort Risikomanagement. Wo ist denn die Risikomanagement-Komponente in diesem Monitoring-System?
Barelmann: Über eine Maske in der Software lassen sich Anlagenteile nach ihrer Priorität kennzeichnen. Mit diesen Informationen berechnet das Programm das Risiko, das dort in Kauf genommen werden kann oder eben nicht. In der neuen Revision der Qualitätsmanagementnorm ISO9001 werden Sie zum Beispiel angehalten, die Risiken für Komponenten und Anlagenabschnitte im Einzelnen zu bewerten. Das lässt sich mit unserer Lösung umsetzen.

Viel wichtiger als externes Wissen ist das Know-how um die eigenen Prozesse, sonst kommen Sie nicht weit.
Dieter Barelmann, Videc

ITP Welche Protokolle lassen sich überwachen?
Barelmann: Wir gehen zur Zeit nicht auf die Protokollebene runter, sondern schauen, wie die Netzwerkteilnehmer miteinander kommunizieren. Unser Fokus liegt auf TCP-Verbindungen. Die meisten Angriffe spielen sich noch immer in klassischen Netzwerken ab. Allerdings haben wir geplant, in einer der nächsten Versionen unserer Lösung Analysefunktionen für gängigen Protokolle zu implementieren.

ITP Wie sieht Ihr Dienstleistungsportfolio aus? Helfen Sie bei der Implementierung des Systems?
Barelmann: Wir leisten natürlich Support und schulen die Anwender auf das Produkt. Alles ist recht einfach gehalten. Wenn Sie ein Netzwerk einrichten können, können Sie auch IRMA betreiben. Viel wichtiger als externes Wissen ist das Know-how um die eigenen Prozesse, sonst kommen Sie nicht weit. *(ppr)*■

www.videc.de