Dieter Barelmann

Cyberangriffe auf kritische Infrastrukturen zuverlässig abwehren

Mit der Einführung des IT-SiG 2.0 gewinnt das Thema Anomalieerkennung in der Leit-, Automatisierungs- und Fernwirktechnik in allen Bereichen absolute Aufmerksamkeit. Gründe dafür sind die zunehmende Frequenz und Komplexität von Cyberangriffen. Maßnahmen zur Angriffserkennung und -reaktion sind entsprechend wichtig und hoch.

Bild 1 Die Netzwerke stets aufmerksam im Blick behalten: Seit 1. Mai 2023 ist die Anomalieerkennung in Einrichtungen der kritischen Infrastruktur Pflicht.

Quelle: Videc

Seit dem 1. Mai 2023 verlangen das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG § 2 Abs. 9b, § 8a Abs. 1) und das Energiewirtschaftsgesetz (EnWG § 11 Abs. 1e) von Betreibern kritischer Infrastrukturen und von Energieverteilungsnetzen ein System zur Angriffserkennung (SzA). In weiteren Schritten werden auch andere Bereiche zu diesen Maßnahmen verpflichtet. Ver- und Entsorgungsunternehmen sind zum Teil jetzt schon betroffen, fallen aber in den kommenden Verpflichtungen ebenfalls unter dieses Gesetz. In der europäischen Gesetzgebung EU NIS2 ist der europäische Rahmen für Betreiber kritischer Infrastrukturen festgelegt. Damit sind die Cyber-Security-Mindeststandards definiert. Die EU NIS2 wird in knapp zwei Jahren verbindlich sein. Das BSI hat eine Orientierungshilfe zum IT-Sicherheitsgesetz 2.0 veröffentlicht, die eine Hilfe bei der Einführung geben soll. Eine Checkliste unter www.videc.de listet die diesbezüglichen Anforderungen über-

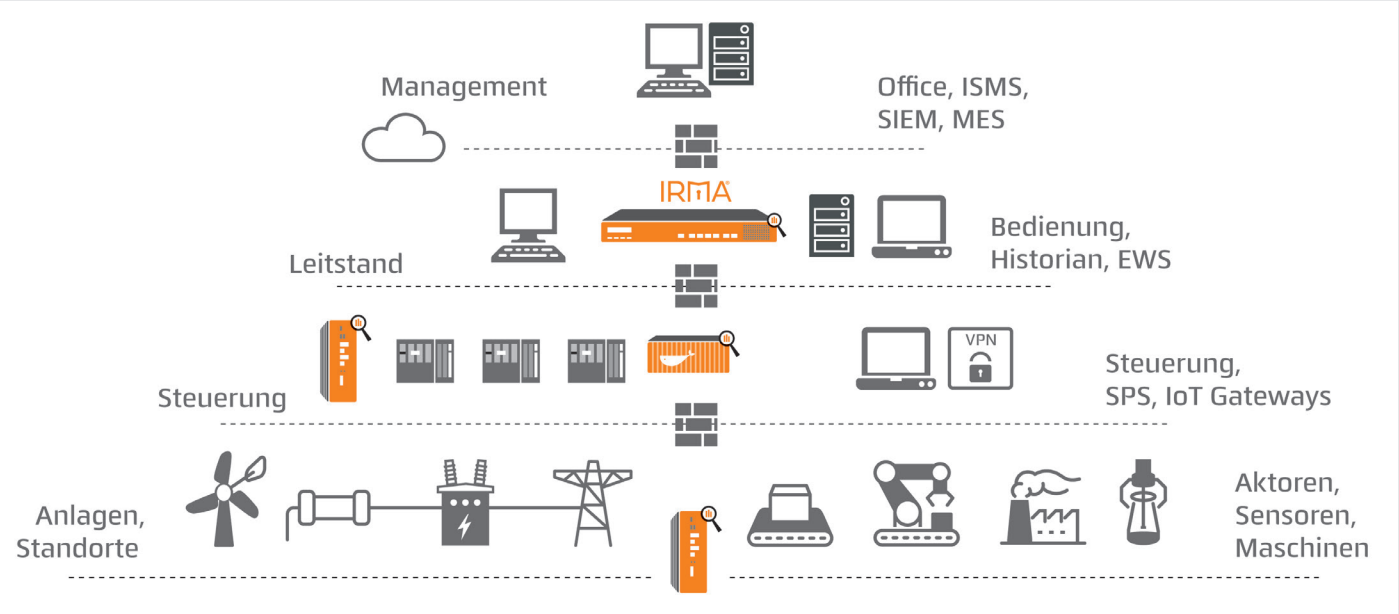


Bild 2 Einordnung von IRMA in die Systemarchitektur
Quelle: Videc

sichtlich auf, sodass sie durch die Verantwortlichen vergleichsweise einfach abzuarbeiten sind.

Blick in die Tiefe erforderlich

Industrielle Cybersicherheitslösungen müssen eine umfassende Übersicht sowie einen tiefen Einblick in die zu überwachenden Anlagen zur Verfügung stellen. Aktuellen Angriffen lässt sich entsprechend der Vielfalt von Geräten und Protokollen – auch sehr alten – nur noch bedingt durch eine Absicherung an den Netzgrenzen begegnen. In den meisten Fällen wird bei direkten Aktivitäten nach dem Vorfall (Incident Response) und fast immer bei der folgenden Analyse klar, dass es Anzeichen im Produktionsnetzwerk gab. Anomalien, also Abweichungen vom Normalbetrieb, sind erste Anzeichen. Eine Angriffserkennung ist Stand der Technik und in der heutigen Zeit ein absolutes Muss für alle automatisierten Anlagen.

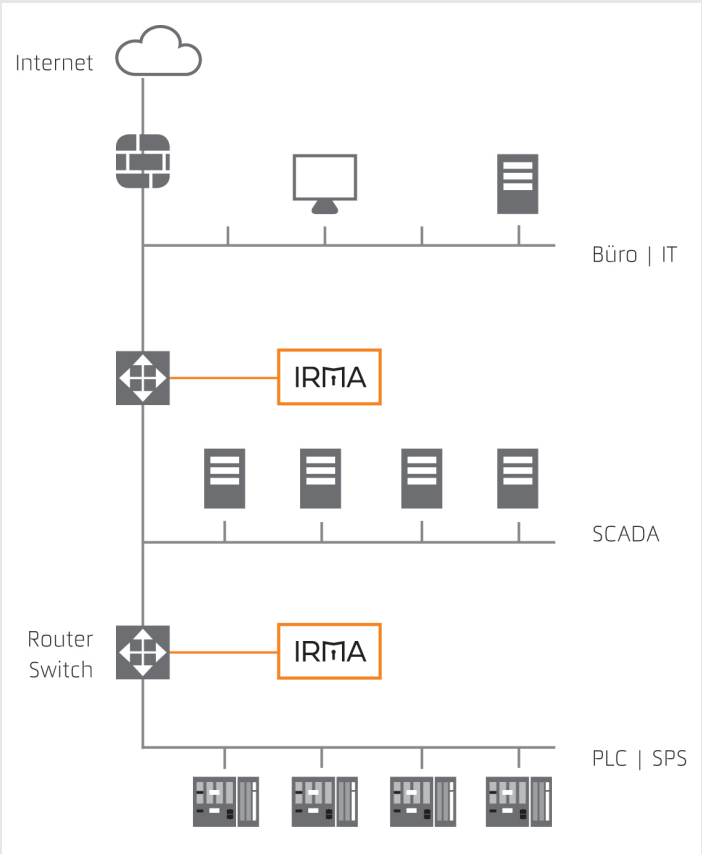
Nichts ist absolut sicher – Angriffserkennung

Sämtliche klassischen Methoden der Security sind nur bedingt sicher. Firewall und Virenschutz können nur einen Teil absichern. Auch eine gekapselte Anlage ist nicht wirklich sicher. Eine Angriffs- oder Anomalieerkennung geht dabei jedoch anders vor. Hier werden die Unregelmäßigkeiten im Netzwerk betrachtet. Sinnvollerweise ist die Angriffserkennung passiv, sie ist nur lesend am Netzwerkrouter angeschlossen und beobachtet sämtliche Kommunikation, ohne das Netzwerk zu belasten.

Die Einrichtung einer Angriffserkennung ist in den ethernetbasierten Netzen schnell erfolgt. Die vollständige Erfassung und Analyse aller Kommunikationspartner, Assets, Zeitpunkte und der Dauer der Kommunikation sowie der gesprochenen Protokolle aller Sitzungen passiert ohne weitere Anpassungen. Alle Teilnehmer werden erkannt und aufgelistet bzw. in einem Netzplan dargestellt.

Alarmierungen erfolgen ohne Konfiguration auf Basis von Anomalien. Anomalien sind dabei einerseits abweichendes Verhalten vom Normalbetrieb (Fingerprint der

Bild 3 Der Platz von IRMA im Unternehmensnetzwerk
Quelle: Videc



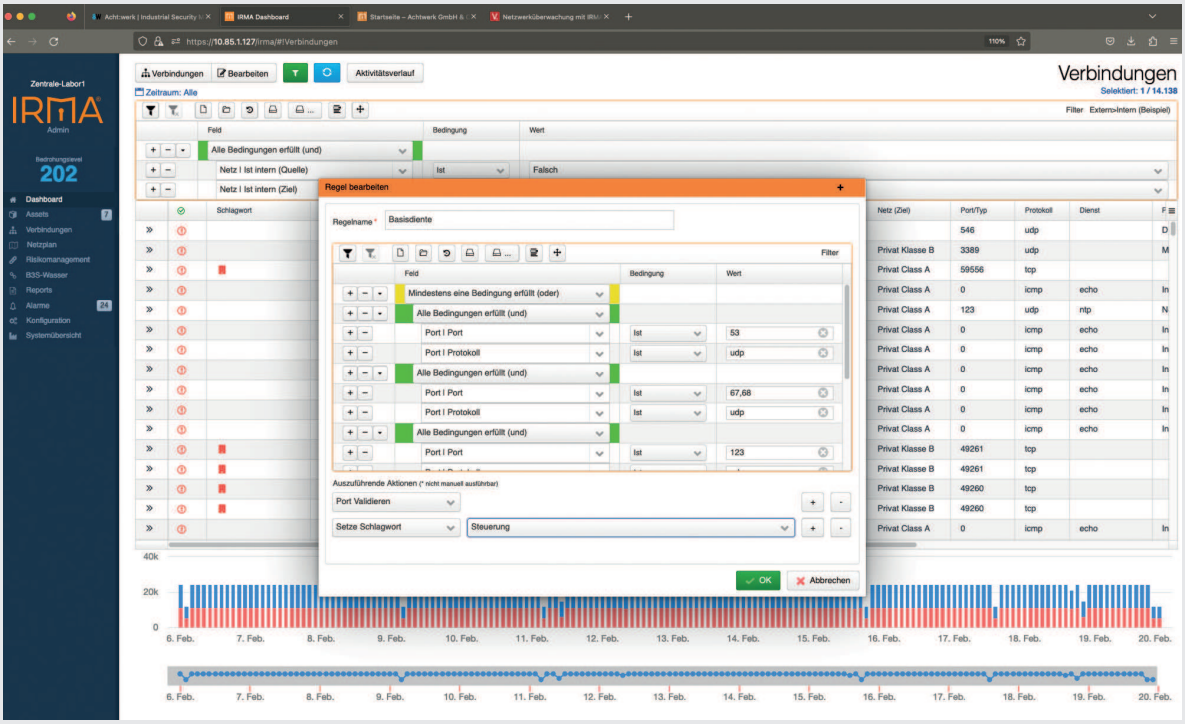


Bild 4 Damit die Anomalieerkennung einem Regelwerk folgen kann, müssen zuvor bestimmte Bedingungen definiert werden.
Quelle: Videc

Anlage). Anderseits sind es auch Protokollfehler und -manipulationen bis hin zur automatisierten Erkennung von Aktivitäten unterschiedlicher Angriffsmodelle.

Eine Detektion bietet indirekten Schutz gegen Angriffe auf das Netzwerk, sie deckt diese frühzeitig auf. Aktuell beträgt die Zeit zwischen Infizierung, also dem Beginn des Angriffs, und dem Schadenseintritt ca. sieben Monate. Diese „Inkubationszeit" kann mit einer Anomalieerkennung effizient genutzt werden, um die entsprechenden Maßnahmen zu treffen. Für die Reaktion (Respond) stehen die aufgezeichneten Daten innerhalb der Alarmierung direkt zur Verfügung und werden für die forensischen Untersuchung gespeichert. Schnell wird klar, ob alle Assets bekannt sind, welche Bedrohungen vorhanden sind und wie die bereits vorhandenen Maßnahmen helfen. Mit einer Anomalieerkennung wirken die Maßnahmen weit vor dem Eintritt eines Notfalls. Der ehemals hohe Aufwand für einen Schutz hat sich durch den Einsatz einer automatisierten Anomalieerkennung stark reduziert. IRMA* (Industrie Risiko Management Automatisierung) wurde als Anomalieerkennung für die Bereiche der Produktion entwickelt. Eine Zielsetzung war dabei, die Security in den Automatisierungsbereichen möglichst einfach mit dem vorhandenen Personal zu bewerkstelligen. Der Pflegeaufwand sollte gering, die Projektierung durch das Anlagenpersonal möglich sein.

So einfach, so sicher!

Security muss übersichtlich, bedienbar und einfach sein. Dieser Anspruch und das Prinzip „Security by Design" bilden die Grundpfeiler für die Entwicklung von IRMA. Das Resultat ist die Erfüllung der Empfehlungen des BSI CS 134 zu „Monitoring und Anomalieerkennung in Produktionsnetzwerken", das IT-Sicherheitsgesetz 2.0 und die Möglichkeit der Nutzung in allen Branchen. Besonderen Wert wurde auf die Branchen Wasser und Abwasser gelegt.

IRMA enthält in der Grundkonfiguration bereits die wichtigsten Kernfunktionen, um die Kritis-Anforderungen der Anomalieerkennung zu erfüllen.

Automatische Erkennung der Assets (Teilnehmer) im Netzwerk

Insgesamt geht es um die Erfassung relevanter Protokolldaten der betreffenden Systeme und Netzwerke, die Aufschluss über einen Cyberangriff geben können. Idealerweise werden eine Deep Packet Inspection für relevante Protokolle (z. B. 104er-Fernwirkprotokoll oder Siemens S7) und speziell entwickelte Algorithmen mit einem effizienten maschinellen Lernen zur Erstellung des Asset-Registers der Produktionsanlage kombiniert. IRMA identifiziert, erfasst und analysiert alle Systeme und Verbindungen vollständig autonom ohne jegliche Aktivität im Netzwerk der Produktionsanlage. Diese grundsätzliche Funktion ist im Wesentlichen passiv, bedeutet aber, dass zunächst kein Teilnehmer aktiv angefragt wird. Ein wichtiger Aspekt, da viele alte Geräte auf solche Abfragen sehr sensibel reagieren und neue Teilnehmer dadurch automatisch erkannt werden. Auch bei segmentierten Netzwerken wird dabei die ganzheitliche Überwachung durch den Einsatz von IRMA-Client-TAPs (verteilte Sensoren) gewährleistet.

Eine Anzeige des Bedrohungslevels in Form eines Wertes gibt dem Anwender einen kontinuierlichen Überblick über den Zustand seiner Anlage. Über die Zeit gesehen, lässt sich über die Kennzahl auch in einer Langzeitbetrachtung bewerten. Das ist ein nützliches Werkzeug für jeden Anlagenfahrer, der mit einem Blick seine Anlage einschätzen und ggf. notwendige Maßnahmen einleiten kann.

Risikomanagement

Das Risikomanagement unterstützt die Mitarbeiter (IT und Automatisierungsfacharbeiter) bei der Bewertung eines jeden Assets und ermöglicht die standardkonforme Dokumentation für das Security-Management. Mit der Bewertung der Risiken lassen sich Maßnahmen optimaler planen und bei Anomalien besser einschätzen. Die Investitionen in die Anlage können somit zielge-

* IRMA – eingetragenes Markenzeichen

richtet dort eingesetzt werden, wo das Risiko am besten reduziert werden kann.

Netzwerkplan

Die grafische Darstellung des gesamten Netzwerkes zeigt alle Querverbindungen in der Kommunikation sowie die Auswertungen zu jedem einzelnen Teilnehmer. Jeder Netzwerkplan kann einzeln gespeichert werden und bei erneuter Öffnung wird der Anwender sofort auf die Änderungen hingewiesen. Er gibt stets eine aktuelle Onlineübersicht über die gesamte Anlage in Form unterschiedlicher grafischer Darstellungen oder auch in Listenform.

Alarmierung

Die Alarmierung zu Anomalien, Änderungen und somit möglichen Angriffen erfolgt in der Bedienoberfläche und automatisiert über gesicherte Verbindungen. Mit der Schaltung von potenzialfreien Kontakten steht eine elektrische Alarmierung direkt im Leitsystem zur Verfügung. Durch die Vielzahl der elektronischen Datenschnittstellen als restAPI, SMTP oder SFTP ist die Weitergabe und Integration in ein Alarmierungssystem (z. B. AIP) oder in unternehmensweite Security-Information-Event-Management(SIEM)-Systeme sowie Information-Security-Management(ISMS)-Systeme aufwandsarm möglich.

Die aktive Suchfunktion

Die Informationen aus dem Datenpool gehen in IRMA grundsätzlich zwei Wege. Zum einen werden die Daten in IRMA analysiert sowie in der IRMA-Weboberfläche übersichtlich und verständlich dargestellt. Bei Anomalien erfolgt eine automatische Alarmierung.

Zum anderen werden alle passiv erfassten Netzwerkpakete in einem Speicherbereich gesichert und stehen im Nachgang für eine forensische Analyse über PCAP-Dateien zur Verfügung.

Mit IRMA steht der Angriffserkennung im Unternehmensumfeld ein intuitiv bedienbares Paket zur Verfügung. Dabei kann der Betreiber seine Sicherheitsaufgaben auch an ein kompetentes Unternehmen auslagern und IRMA als Sensor für die Datenbeschaffung und Alarmierung verwenden.

Eine SIEM-Integration mittels der integrierten Rest-API ist ohne Probleme möglich. In solch einer Konstellation liefert IRMA die notwendigen Daten für ein übergeordnetes System.

Die Produktentwicklung in Bremen folgt den Prinzipien des Security by Design (vgl. IEC 62443-4-x). Die Entwicklungsmannschaft besteht aus einem Team kompetenter IT-/OT-Sicherheitsexperten, die auf mehrere Jahrzehnte Berufserfahrung in den Marktsegmenten IT-Security und Automatisierung zurückblicken können. IRMA ist durch die Selbstverpflichtungserklärung bereits seit vielen Jahren Trägerin des TeleTrusT-Vertrauenszeichens „IT Security made in Germany".

Bedrohungslage und Umsetzung in der Branche Wasser/Abwasser

Die Bedrohungslage ist weiterhin sehr hoch und immer noch steigend. Bisherige Meldungen zu Hacks einzelner Anlagen bleiben mittlerweile aus, da auch die Anzahl der Meldungen sehr hoch ist und auch nicht alle Angriffe gemeldet bzw. bekannt werden. Für die betroffenen Unternehmen sind die Kosten der Wiederherstellung um einiges höher als die Vorsichtsmaßnahmen und bedeuten im Nachgang eine mehr als doppelt so hohe Investition.

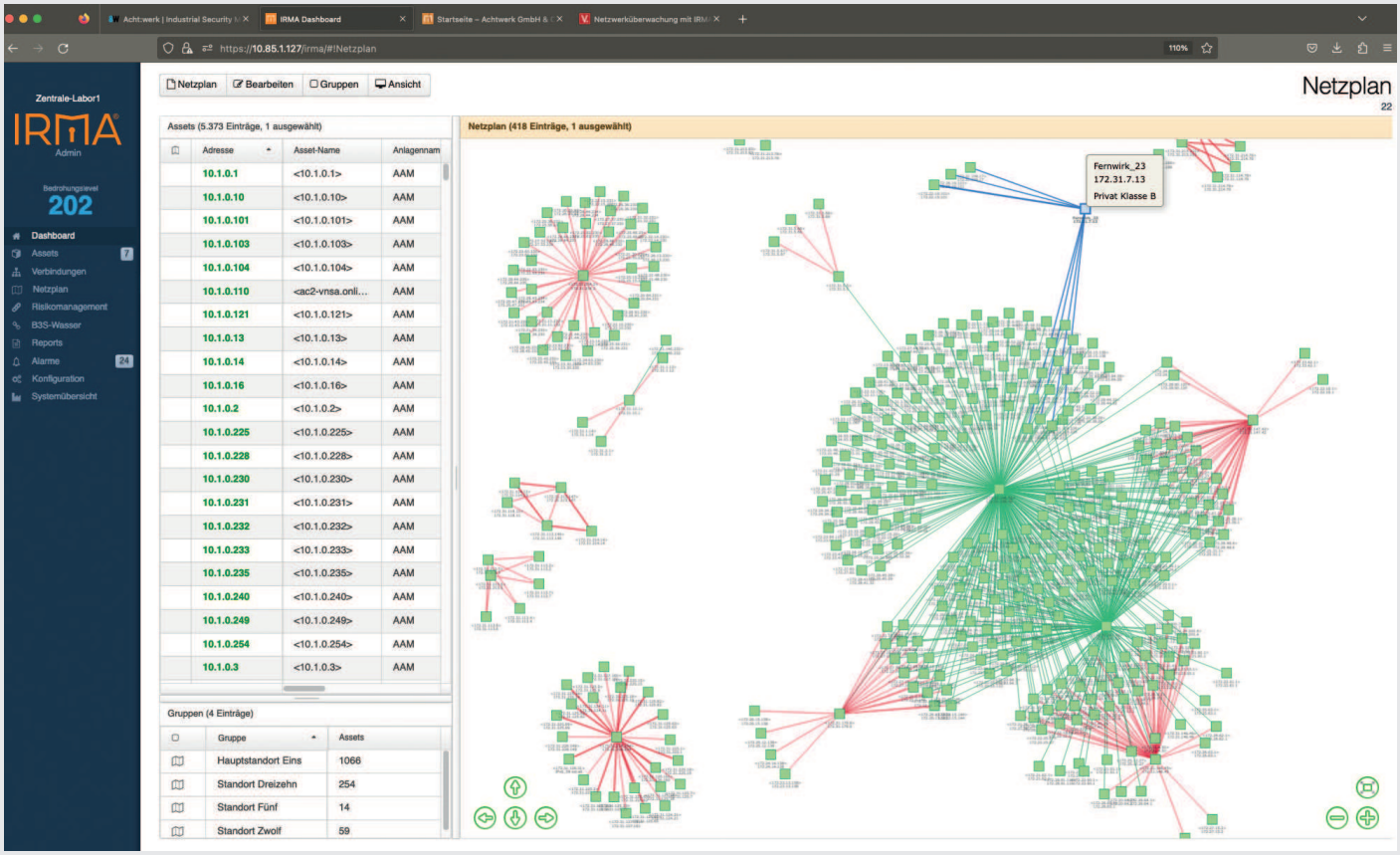


Bild 5 Ansicht eines typischen Netzwerkplans

Quelle: Videc

Um eine Anlage versichern zu können, muss ein Nachweis über die getroffenen Maßnahmen erfolgen. Ohne entsprechende Vorkehrungen geht kaum noch eine Versicherung auf das Risiko ein.

Für jedes gehackte Unternehmen ist es allerdings auch wichtig zu wissen, dass vom Befall bis zum Ausbruch im Mittel derzeit ca. 170 Tage vergehen. Man muss nur die Mechanismen besitzen, den Befall zu bemerken.

Die Umsetzung dafür ist eher schleppend. Seit ca. 5 Jahren kommuniziert Videc das Thema. Lediglich die unter Kritis fallenden Unternehmen/Verbände/Anlagen sind auf dem Weg etwas zu unternehmen. Die Problematik liegt zum Teil in den Budgets, zum Teil beim fehlenden Personal bzw. Know-how.

Ausgesprochen positiv sind die Rückmeldungen der Unternehmen, die mit der Umsetzung begonnen haben. Zielführend für eine sinnvolle Orientierung sind die kostenlosen Einführungsseminare, die in diversen Städten von Videc angeboten werden.

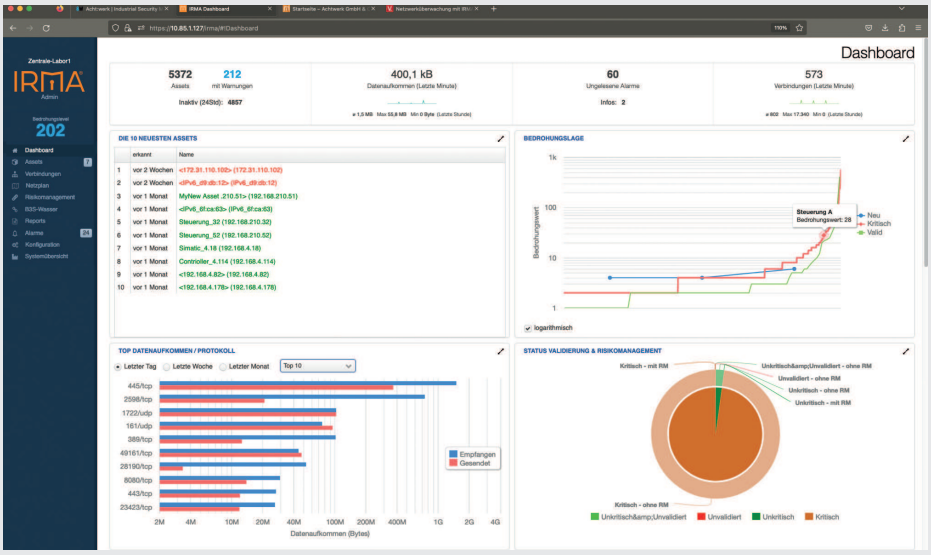


Bild 6 Das Dashboard verschafft einen schnellen Überblick über relevante Aktivitäten im Netzwerk.

Quelle: Videc

Eine Umsetzung solch komplexer, neuer Themen scheint in dem Zeitraster bis zum 1. Mai 2023 eher schwierig zu sein. Zudem ist das Thema OT Security in vielen Bereichen der Automatisierung noch nicht vollends angekommen.

■ ***Dieter Barelmann***
Geschäftsführer
VIDEC Data Engineering GmbH
dbarelmann@videc.de
www.videc.de