Fraunhofer
IAIS

FRAUNHOFER-INSTITUT FÜR INTELLIGENTE ANALYSE- UND INFORMATIONSSYSTEME IAIS

UND ES GEHT DOCH ...

360° CHECK INDUSTRIAL SECURITY

… FRAUNHOFER IAIS

Operation Technology ist angreifbar

Moderne Industriesysteme und Produktionsanlagen (Operation Technology, OT) sind heute immer weiter vernetzt und tauschen Daten mit anderen Systemen aus. Die Software der Maschinen wird durch den Hersteller regelmäßig aktualisiert. Updates erfolgen entweder durch einen Servicetechniker vor Ort oder aber »over the air«. Daten der Maschinen werden in Echtzeit an Analysesysteme übertragen und ausgewertet. Das klassische Air-Gap zur Isolation der Operation Technology funktioniert heute nicht mehr als Sicherheitsmaßnahme. Durch die Nähe zu anderen IT-Systemen und häufigen Softwareänderungen nehmen Risiken für einen Ausfall von Produktionsanlagen immer weiter zu.

Vernetzung lässt sich nicht aufhalten

Die Anforderungen moderner Operation Technology in Bezug auf Vernetzung und Datenaustausch werden in Zukunft immer weiter zunehmen. Entwicklungen, die unter den Begriffen Industrie 4.0 oder Internet of Things (IoT) zusammengefasst werden, tragen hierzu weiter bei. Der Einsatz von Big-Data- und Analytics-Systemen ermöglicht einen optimierten Betrieb der Produktionsanlagen. Verfahren wie Predictive Maintenance und Predictive Monitoring reduzieren Fehler und minimieren die Ausfallzeiten der Anlagen.

Hohe Verfügbarkeit hat Priorität

In Sicherheitsfragen gibt es deutliche Unterschiede zwischen den Anforderungen der klassischen Office IT und der Operation Technology. Die Kernaspekte von IT-Sicherheit sind Vertraulichkeit der Daten, Daten-Integrität und Verfügbarkeit der Systeme. Für die Operation Technology ist der Aspekt der Verfügbarkeit enorm wichtig. Der Ausfall von Produktionsanlagen kann schon nach kurzer Zeit kritische Auswirkungen für das Gesamtunternehmen haben. Dies muss bei der Entwicklung einer Sicherheitsstrategie berücksichtigt werden. Maßnahmen und Vorgehensmodelle aus der IT-Security können nicht eins-zu-eins auf die OT-Security übertragen werden.

Sichere Vernetzung von IT und OT

Aufgrund der unterschiedlichen Anforderungen und der dennoch erforderlichen Vernetzung muss eine gemeinsame Sicherheitsstrategie für die Operation Technology und die klassische Office-IT entwickelt werden. Wir bieten Ihnen mit unserem 360° Check Industrial Security eine praxisnahe Analyse Ihrer IT- und Systemlandschaft. Wir identifizieren die bestehenden Risiken, bewerten diese und entwickeln mit der Security Strategy konkrete Maßnahmen zur Risikoreduzierung.

UND ES GEHT DOCH – FRAUNHOFER IAIS

Innerhalb des Fraunhofer IAIS arbeiten IT-Spezialisten, Sicherheitsexperten und Ingenieure eng zusammen. Unser Angebot kombiniert langjährige Praxiserfahrung im Sicherheitsumfeld mit neuesten technologischen Entwicklungen. Abgestimmt auf Ihre Anforderungen unterstützen praxiserfahrene Berater Sie sowohl bei einzelnen fachlichen Problemstellungen als auch bei der Realisierung innovativer Konzepte und darauf aufbauender Projekte.

360° CHECK

Bei unserem 360° Check berücksichtigen wir mit der von uns entwickelten TAM-Methodik alle entscheidenden Faktoren, ohne zu sehr ins Detail zu gehen. In der Analyse werden die folgenden Aspekte berücksichtigt:

- Architektur und Strategie der Information Technology
- Systemlandschaft der Operation Technology
- Ressourcen und Wertschöpfungskette
- Schnittstellen und Abhängigkeiten
- Sicherheitskonzepte, Krisenmanagement

RISIKOBEWERTUNG

Der 360° Check bildet die Grundlage für eine individuelle Analyse und Bewertung der Risiken für Ihre IT und OT. Im Rahmen dieser Risikoanalyse werden unter anderem folgende Fragen beantwortet:

- Wie komplex sind die Abhängigkeiten zwischen IT und OT?
- Ist die Operation Technology ausreichend geschützt?
- Können kritische Vorfälle frühzeitig erkannt werden?
- Sind die Krisennotfallpläne ausreichend?
- Ist eine Awareness zu Sicherheitsrisiken im gesamten Unternehmen etabliert?

INDUSTRIAL SECURITY STRATEGY

Wir entwickeln für Ihr Unternehmen eine individuelle Industrial Security Strategy. Dabei werden sowohl die Anforderungen der Office-IT als auch die der Operation Technology berücksichtigt. Es werden technische und organisatorische Maßnahmen zur Minimierung der existierenden Risiken entwickelt. Im Fokus steht dabei eine Widerstandskraft gegen kritische Situationen aufzubauen. So ist es möglich auch bei Störfällen weiter handlungsfähig zu sein, diese so schnell wie möglich zu beheben und den potentiellen Schaden so gering wie möglich zu halten. Bei der Entwicklung der Industrial Security Strategy gehen wir folgendermaßen vor:

- Szenarienbasierte Priorisierung der existierenden Risiken
- Entwicklung eines gemeinsamen Sicherheitskonzeptes für Office-IT und Operation Technology
- Sicherheitskonzepte für besonders kritische Systeme
- Krisenmanagementplan für wichtige Prozesse

UMSETZUNG

Wir unterstützen und begleiten Sie gerne bei der Umsetzung der Strategie. Dazu bieten wir die Erarbeitung einer Roadmap, die Technologie- und Zulieferer-Auswahl sowie eine Unterstützung beim Change Management.

Fraunhofer-Institut
für Intelligente Analyse- und
Informationssysteme IAIS

Schloss Birlinghoven
53757 Sankt Augustin

Adaptive Reflective Teams
Ansprechpartner: Sebastian Müller
Telefon +49 2241 14-2562
Fax +49 2241 14-2342
sebastian.mueller@iais.fraunhofer.de

www.iais.fraunhofer.de
www.iais.fraunhofer.de/art

www.iais.fraunhofer.de/industrial-security