Funktionale Sicherheit und Cybersecurity ganzheitlich betrachten.

Mehr denn je benötigt die Industrie heute eine neue Art des Denkens und Handelns, die die potentiellen Bedrohungen frühzeitig erkennt und ihnen wirksam begegnet. Cybersecurity ist bereits ein integraler Bestandteil der modernen Technologie und eine unabdingbare Voraussetzung für die Sicherheit industrieller Anlagen. Industrielle Sicherheit ohne IT-Sicherheit wird es nicht mehr geben.

Wir haben im Nachfolgenden die unseren Experten häufigsten gestellten Fragen zusammengestellt und beantwortet.

WIE WIRKEN SICH CYBERSECURITY-BEDROHUNGEN AUF DIE FUNKTIONALE SICHERHEIT AUS?

Mit dem technologischen Fortschritt nehmen immer mehr Industrieanlagen IP-basierte Lösungen an. Dies kann ihre Anfälligkeit für Cybervorfälle oder Störungen erhöhen. Wir haben bereits gezielte Angriffe auf sicherheitsinstrumentierte Systeme (SIS) erlebt, wie z.B. mit dem TRITON-Angriff, und wir werden in Zukunft wahrscheinlich noch weitere erleben. Glücklicherweise waren die Angreifer im Fall TRITON nicht erfolgreich, da das Sicherheitssystem erfolgreich reagierte. Sicherheitsnormen, wie die IEC 61508, verlangen nun, dass Cybersecurity-Risiken als Teil der allgemeinen Sicherheits-bewertung angesehen werden.

www.tuv.com/fscs-de

TÜVRheinland®
Genau. Richtig.

WIE WIRD FUNKTIONALE SICHERHEIT UND CYBERSECURITY INNERHALB EINES UNTERNEHMEN AUSGEWOGEN BERÜCKSICHTIGT?

Die Ergebnisse unserer Studie zur industriellen Sicherheit sowie die der Cybersecurity Trends 2020 zeigen, dass Funktionale Sicherheit und Cybersecurity untrennbar miteinander verbunden sind. Um Sicherheits- und Cybersecurity-Anforderungen zu erfüllen, sollte ein risikobasierter Ansatz gewählt werden. Somit, wird sichergestellt, dass begrenzte Budgets für die wichtigsten Sicherheits- und Cybersecurity-Bereiche ausgegeben werden. Dies erfordert von OT-Managern ein detailliertes Verständnis von Geschäfts-, Cybersecurity- und Sicherheitsrisiken, um die Budgets auch entsprechend zu priorisieren.

WIE HOCH SIND DIE INVESTITIONEN FÜR AUSREICHENDE CYBERSECURITY-MASSNAHMEN?

Dies hängt vom Geschäftsrisiko ab. Eine Bewertung sollte anhand eines objektiven Rahmens, wie dem NIST Cybersecurity Framework oder IEC 62443 vorgenommen werden. Diese geben einen sehr guten Überblick über Fragen zum Geschäftsrisiko sowie über fehlende oder unzureichende Cybersecurity-Kontrollen. Jede Investition in Cybersecurity-Maßnahmen muss im Verhältnis zum Risiko stehen. Es sollte ein Programm erstellt werden, das sich zuerst mit den Schlüsselfragen und im Anschluss mit den verbleibenden Fragen befasst. Es ist unwahrscheinlich, dass dies in einem einzigen Schritt möglich ist. Abhängig vom individuellen Geschäft und den bestehenden Cybersecurity-Stufen, kann ein effektives Programm 2 bis 3 Jahre dauern. Risikobewertungen sollten regelmäßig durchgeführt werden, um somit die sich ständig ändernde Art und Weise von Cybersecurity-Bedrohungen erkennen und meistern zu können.

WAS SIND DIE GRÖSSTEN HERAUSFORDERUNGEN IM BEREICH DER INDUSTRIELLEN SICHERHEIT?

Für viele Firmen ist die größte, und bisher von vielen noch unterschätze Herausforderung, die notwendige organisatorische und kulturelle Veränderung die Unternehmen in Angriff nehmen müssen. Neue IP-gestützte Technologien können die Anlageneffizienz massiv verbessern. Allerdings sind sie oft mit Risiken verbunden, die möglicherweise nicht berücksichtigt wurden. Hinzukommt, dass auf Grund des Fachkräftemangels es für Unternehmen schwierig ist ausgebildetes Personal zu finden, die die industriellen Prozesse, die Betriebstechnik und Cybersecurity verstehen.

IST ES BESSER IT-MITARBEITER ODER EXPERTEN FÜR INDUSTRIELLE PROZESSE ALS OT-CYBERSECURITY-SPEZIALISTEN WEITERZUBILDEN?

Es ist möglich IT-Mitarbeiter zu OT-Cybersecurity-Experten weiterzubilden, wenn sie ein Verständnis für industrielle Prozesse, Ingenieurwesen und eine Leidenschaft für das Thema besitzen. In der Praxis sollte das optimale OT-Cybersecurity-Team aus IT-Mitarbeitern, OT-Prozessingenieuren, Anlagenbesitzern und Cybersecurity-Experten bestehen. Dieser Ansatz ermöglicht einen Austausch unter den Experten, wodurch Wissen und Erfahrung im Team geteilt werden. TÜV Rheinland Akademie bietet Coaching und Weiterbildungen für Ihre Teammitglieder an, um den Aufbau dieser Fähigkeiten zu unterstützen.

WAS IST DER BESTE WEG, UM DIE EXPERTISE EINES CHIEF INFORMATION SECURITY OFFICER / CHIEF SECURITY OFFICER FÜR IT UND OT IM UNTERNEHMEN ZU BÜNDELN, UM AKTUELLE RISIKEN UND ANGRIFFE ZU MINIMIEREN?

Es bedarf langjähriger Erfahrung, um sich die notwendige Expertise in Cybersecurity, IT und OT zu erarbeiten. Bei dem Wissens- und Erfahrungsaufbau sollte die Einbindung Dritter, wie TÜV Rheinland, in Betracht gezogen werden. TÜV Rheinland kann als Partner bei langfristigen Mitarbeiterschulungen in Cybersecurity und den damit verbundenen Technologien und Herausforderungen unterstützen.

SOLLTE ES IN EINEM UNTERNEHMEN EINEN SEPARATEN OT-SPEZIFISCHEN CHIEF SECURITY OFFICER (CSO) GEBEN?

Dies hängt vom jeweiligen Unternehmen ab. Viele Organisationen gehen zu einem konvergierenden Ansatz über, bei dem IT- und OT-Cybersicherheitsteams eng zusammenarbeiten und ein zentraler CSO verantwortlich ist. Das Problem ist, dass ein solcher CSO-Experte schwer zu finden ist, so dass es mittelfristig wahrscheinlich besser ist, getrennte Funktionen zu haben.

WAS SIND DIE WICHTIGSTEN FAKTOREN BEIM SCHUTZ VON OT-UMGEBUNGEN GEGEN RANSOMWARE?

Ransomware ist eine schädliche Software, durch die Computersysteme verschlüsselt werden. Häufig über eine Phishing-E-Mail zugestellt, verlangt der Angreifer Zahlungen für die Entschlüsselung der Daten. Selbst wenn das geforderte Geld bezahlt wird, kann der Entschlüsselungsprozess oft fehlschlagen. Da IT- und OT-Systeme oft miteinander verbunden sind,

kann es nach einem Ransomware-Vorfall zu direkten Auswirkungen auf eine Produktionsanlage kommen, der zu Produktions- und Systemausfallzeiten führt.

Patching, gute Backups und ein segmentiertes Netzwerk sind Maßnahmen, um Ransomware zu verhindern, ebenso wie eine gute Benutzerschulung, E-Mail-Filterung und -Verwaltung. OT-Assets müssen dokumentiert und vollständig verstanden werden, ebenso wie ihre Verbindung zu IT-Systemen. Die Verwendung richtig konfigurierter Firewalls kann dabei hilfreich sein. Letztendlich ist die Antwort auf einen erfolgreichen Ransomware-Angriff die Wiederherstellung von Systemen aus dem Backup. OT-Systeme müssen ebenfalls im Backup abgesichert sein. Damit das Backup versehentlich nicht durch dieselbe Ransomewre verschlüsselt wird, ist es notwendig es vor Angriffen zu schützen. Für den Fall, dass Sie Opfer eines Ransomeware-Angriffs werden, wird ein guter und gut eingespielter Reaktions- und Wiederherstellungsplan sicherstellen, dass Sie über die Personen, Prozesse und Technologien verfügen, um mit dem Angriff umzugehen.

WIE KANN DAS RISIKO MIT EXTERNEN DIENSTLEISTERN / DRITTEN MINIMIERT WERDEN?

Bei Dritten ist es wichtig, die Haftung zu definieren und sicherzustellen, dass diese durch entsprechende Verträge abgesichert ist. Cybersecurity muss von Beginn an in einer Lieferantenbeziehung berücksichtigt werden, d.h. schon vor der Vertragsunterzeichnung. Danach sind regelmäßige Audits durch Dritte von größter Bedeutung, um zu überprüfen, ob die Cybersecurity-Maßnahmen während der gesamten Vertragslaufzeit eingehalten werden. Das TISAX-Auditprogramm in der Automobilindustrie zeigt, wie solche Programme zur Cybersecurity-Gewährleistung ablaufen. Es ist ein Bewertungs- und Austauschmechanismus für die Informationssicherheit und ermöglicht die gegenseitige Akzeptanz der Cybersecurity-Bewertungsergebnissen zwischen den Teilnehmern. Wenn Sie sensible Informationen Ihrer Kunden verarbeiten oder die Informationssicherheit Ihrer eigenen Lieferanten bewerten wollen, unterstützt Sie TISAX dabei, den Aufwand zu reduzieren.

IN WELCHEM ZUSAMMENHANG STEHEN GESCHÄFTLICHE RISIKOBEDENKEN UND OT-CYBERSECURITY-RISIKEN?

OT-Systeme sollten in die **G**overnance, **R**isiko und **C**ompliance-Strategie (GRC) des Unternehmens integriert werden, sodass Cybersecurity-Maßnahmen mit anderen wichtigen Geschäftsrisiken berücksichtigt werden.

Wir haben eine neue Systemlösung CARM (Continuous Adaptive Risk Monitoring) entwickelt, die ein GRC-Overlay für OT-Operationen bietet. Sprechen Sie uns an, um weitere Informationen zu erhalten.

WIE WICHTIG IST DER VERLUST VON OT-DATEN WÄHREND EINES ZWISCHENFALLS ODER ANGRIFF? WAS SIND DIE FOLGEN EINES PRODUKTIONSAUSFALLS?

Der Schutz der Verfügbarkeit von Produktionssystemen ist neben dem Schutz von Mensch und Umwelt in der Regel das Hauptanliegen der in diesem Bereich tätigen OT-Cybersicherheitsexperten. Die finanziellen Folgen eines Produktionsausfalls sind in der Regel immens und können einem Unternehmen langfristig schaden. Der OT-Datenverlust darf dabei nicht unbeachtet bleiben. Beispielsweise können OT-Prozessinformationen, Funktionsblockdiagramme oder Unternehmensgeheimnisse dabei verloren oder sogar gestohlen werden, wodurch es zu Reputationsschäden oder Auftragsverlusten kommen kann. Da diese beiden Aspekte von großer Bedeutung sind, ist es wichtig, dass Cybersecurity-Kontrollen und –prozesse eingerichtet werden, um einem unvermeidlichen Angriff oder Zwischenfall meistern zu können.

AN WELCHEM PUNKT FINDET DER ÜBERGANG VON IT ZU OT INNERHALB EINES KOMPLEXEN INDUSTRIELLEN UMFELDS STATT?

Der Übergabepunkt zwischen IT und OT hängt von der Struktur des jeweiligen Unternehmens oder OT-Systems ab. Das Purdue Referenzmodell bietet eine gut Möglichkeit, dies zu erklären. Häufig findet der IT/OT Übergang ab Level 3 oder 4 des-Modells statt. Systeme des 4. Levels befassen sich in der Regel mit dem laufenden Geschäftsbetrieb und sind von den Prozess-Leveln abgekoppelt. In Level 3 befindet sich das Operations Management, welches zu Level 2, der Supervisory Control abgegrenzt ist. Zukünftig und im Zuge der Entwicklung der OT-Welt könnte die Verwendung des Purdue-Modells in Frage gestellt werden. Im Augenblick bietet es aber eine nützliche „Ideal“ -Struktur.

IHRE FRAGE WAR NICHT DABEI? DANN KONTAKTIEREN SIE JETZT EINEN UNSERER EXPERTEN FÜR FUNKTIONALE SICHERHEIT & CYBERSECURITY.

ONLINE KONTAKT

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln, Deutschland
cybersecurity@tuv.com

www.tuv.com/fscs-de

TÜVRheinland®
Genau. Richtig.