Teil1 – Kurzbericht

Vorhaben

Start-Up Secure: Software zur Unterstützung der Entwicklung von cyber-sichereren Industrieprodukten

Die zunehmende Komplexität von Industrieprodukten führt zu unsicheren Produkten und macht automatisierte Prozesse und den Einsatz von Algorithmen zu einer absoluten Notwendigkeit. Daraus ergibt sich die Aufgabe, den Entwicklungsprozess abzusichern, Sicherheitswerkzeuge zu implementieren und die Komplexität zu beherrschen. Angesichts des zunehmenden Mangels an ausgebildeten Sicherheitsexperten und der Zunahme von Cyberangriffen ist dies der einzige Weg, um sichere Industrieprodukte zu gewährleisten.

In der Automobilindustrie sind Fahrzeuge zunehmend von Software abhängig, insbesondere bei selbstfahrenden Autos und Fahrerassistenzsystemen. Da diese Fahrzeuge keine geschlossenen Systeme mehr sind, muss die gesamte Fahrzeugelektronik unter Sicherheitsaspekten betrachtet werden, um sie vor Cyber-Angriffen zu schützen. Die Primary Target GmbH bietet ein Software-Tool zur Automatisierung von Threat Assessments und Remediation Analyses (TARAs) sowie zur Unterstützung bei der Einhaltung von Standards wie NIST, ISO 21434 oder dem ASIL-Standard (Automotive Safety Integrity Level definiert durch ISO 26262). Wichtig ist dabei die Integration von Sicherheitsmaßnahmen in den gesamten Entwicklungsprozess, einschließlich der Zusammenarbeit mit allen Abteilungen und Zulieferern.

Bedrohungen in einem Fahrzeugsystem sind potenzielle Sicherheitsprobleme wie unbefugter Zugriff, Manipulation oder Fehler, die die Sicherheit des Systems gefährden können. Schwachstellen sind dagegen konkrete Schwächen im Systemdesign oder in der Implementierung, die von Angreifern ausgenutzt werden können, wie z. B. nicht aktualisierte Software oder schwache Passwörter. Die Beseitigung dieser Bedrohungen und Schwachstellen ist entscheidend für die Sicherheit und Zuverlässigkeit von Fahrzeugsystemen.

Die Produktidee wurde 2021 in Zusammenarbeit mit Automobilzulieferern und OEMs entwickelt. Die Zusammenarbeit dauert bis heute an und bildet die Grundlage für die Spezifikation der Automatisierung des Entwicklungsprozesses zur Implementierung von Cybersicherheitsregeln und -tests. Während dieser Zeit wurde Oscar Angress, einer der Gründer, von der ISO-Gruppe kontaktiert, um sie bei der Cyber Security ISO 21434 Norm zu unterstützen. Nach einem Markt-Screening haben wir uns entschieden, eine Lösung zu entwickeln, die den manuellen Prozess auf Basis von Excel-Tabellen ersetzt. Im Oktober 2021 begannen wir mit den Vorbereitungen und im Januar 2022 gründeten wir das Unternehmen. Die Entwicklung begann mit einem externen Team, das 2023 durch eigene Mitarbeiter ersetzt wurde. Die Entwickler sitzen in Deutschland, der Ukraine, Pakistan und Australien. Heute verfügen wir über eine frühe Version der Software und haben mündliche und schriftliche Absichtserklärungen erhalten, während wir die Lösung bei Zielkunden demonstriert haben, für die wir Cybersicherheitsdienstleistungen erbringen, wie z.B. Rheinmetall AG (6,4 Mrd. € Umsatz und 26.000 Mitarbeiter), ZF (44 Mrd. € Umsatz und 165.000 Mitarbeiter), VW, Schaeffler (14 Mrd. € Umsatz und 82.000 Mitarbeiter), Panasonic, Continental, Aptiv und andere.

Die Primary Target GmbH ist ein IT-Sicherheitsunternehmen mit 12 Mitarbeitern und Sitz in München. Die 9 Sicherheitsexperten und Programmierer entwickeln eine Softwareplattform zur Absicherung und Automatisierung des Entwicklungsprozesses und der Bedrohungsanalyse von Fahrzeugen. Die ISO 21434 ist die Grundlage für ein Gesetz, das die Bedrohungsanalyse ab dem 8.7.2024 für alle Automobilhersteller und -zulieferer verpflichtend macht. Das Softwaretool ermöglicht es Unternehmen, ihre Prozesse so früh wie möglich im Entwicklungszyklus abzusichern und mögliche Cyberangriffe und Bedrohungen auf Soft- und Hardwarekomponenten automatisch zu erkennen, Risiken zu bewerten und potenzielle Angriffsvektoren zu identifizieren. Dies sichert den Entwicklungszyklus ab, verkürzt Testzyklen, reduziert Zeit und Kosten und unterstützt den Produktionsprozess über alle Abteilungen und Lieferketten hinweg.

Die Lösung besteht aus zwei Komponenten, einer Datenbank mit Komponenten und zugehörigen Angriffsvektoren und einer Prozessplattform. Über diese werden Zugriffsrechte vergeben, verwaltet und kontrolliert. Die zeitliche Versionierung der Bedrohungsanalyse des Entwicklungsstandes wird erfasst und eine gefahrengerechte Ablage und Verschlüsselung der Daten vorgenommen.

Wir haben Algorithmen und Verfahren entwickelt, um Cyber-Bedrohungen zu identifizieren und eine Risikobewertung durchzuführen. Dabei handelt es sich um Verfahren zur Identifizierung von Gegenmaßnahmen gegen potenzielle Bedrohungen eines Datensystems und eine entsprechende Prozessplattform zur Identifizierung von Schutzmaßnahmen. Eine Bedrohung und eine Gegenmaßnahme können mit sieben Attributen zur Durchführbarkeit der Bedrohung und der Gegenmaßnahme versehen werden (z.B. Angriffsvektor, Komplexität, Berechtigungen, Benutzerinteraktion, Reproduzierbarkeit, Ausrüstung und Wahrscheinlichkeit). Alle benötigten Informationen werden aus der selbst entwickelten Datenbank abgerufen, die jeweils Ziele der Cyber-Sicherheit definiert, wobei die potenziellen Bedrohungen einem oder mehreren Attributen zugeordnet werden, die jeweils einen Grad der Durchführbarkeit angeben, der das durch die jeweilige potenzielle Bedrohung auferlegte Sicherheitsrisiko ausgleicht.

Dafür haben wir ein europäisches Patent angemeldet. In einem zweiten Schritt sind die USA, Japan und China geplant. Die Algorithmen und Verfahren wurden programmtechnisch umgesetzt, um die Bedrohungsanalyse und Risikobewertung zu automatisieren. Details dürfen wir nicht veröffentlichen, aber Auszüge aus den Patentschriften sind im Abschlussbericht enthalten.

Von CodeX unterstützter Prozess zur Erstellung einer Bedrohungsanalyse:

1. Definieren Sie den „Anwendungsbereich“: Bestimmen Sie die Systeme und Komponenten im Fahrzeug, die bewertet werden müssen. Dies könnte zum Beispiel das Motorsteuergerät, das Infotainmentsystem, drahtlose Kommunikationssysteme und andere Steuermodule umfassen.
2. Potenzielle Bedrohungen identifizieren: Identifizieren Sie die potenziellen Bedrohungen, denen diese Systeme ausgesetzt sein könnten, z. B. Cyber-Angriffe, physische Manipulation oder andere mögliche Angriffe.
3. Bestimmung der Wahrscheinlichkeit jeder Bedrohung: Bewertung der Wahrscheinlichkeit des Eintretens jeder identifizierten Bedrohung und Einstufung nach Schweregrad.
4. Bewertung der Auswirkungen jeder Bedrohung: Bestimmen Sie die potenziellen Auswirkungen, die jede Bedrohung auf das Fahrzeug und seine Insassen haben kann. Dazu können Sicherheitsrisiken, Datenschutzverletzungen oder finanzielle Verluste gehören.
5. Entwicklung von Strategien zur Risikominderung: Entwickeln Sie Strategien zur Risikominderung für jede identifizierte Bedrohung, z. B. die Implementierung von Sicherheitsprotokollen, die Erhöhung physischer Sicherheitsmaßnahmen oder die Aktualisierung von Software und Firmware.
6. Implementierung von Abhilfestrategien: Implementierung der in Schritt 5 identifizierten Abhilfestrategien und Sicherstellung, dass sie ordnungsgemäß in die Fahrzeugsysteme integriert sind.
7. Prüfung der Wirksamkeit der Abhilfestrategien: Prüfung der Wirksamkeit der Abhilfestrategien durch Penetrationstests und andere Sicherheitsbewertungen, um sicherzustellen, dass sie wie vorgesehen funktionieren.
8. Überwachung und Aktualisierung: Kontinuierliche Überwachung der Fahrzeugsysteme auf potenzielle Bedrohungen und Aktualisierung der Schutzstrategien nach Bedarf.
9. Dokumentation des Prozesses: Dokumentation des gesamten Prozesses, einschließlich der Bewertung, der Korrekturstrategien und der Testergebnisse, um eine klare Aufzeichnung des Sicherheitsstatus (TARA) des Fahrzeugs zu erhalten.

CodeX wird ab dem 4. Quartal 2024 implementiert und an Kunden im Automobilmarktsegment verkauft. Über unsere 9 laufenden Serviceverträge zur Erstellung von Bedrohungsanalysen und frühere Kundenkontakte sind wir in Gesprächen mit OEMs und großen Zulieferern. Parallel dazu wird unsere CodeX-Bedrohungsdatenbank so angepasst, um auch andere vertikale Märkte zu adressiert, die etwa fünfmal so groß sind wie der Fahrzeugmarkt.

Die Pipeline wurde durch Veranstaltungen, an denen wir teilgenommen haben, öffentliche Präsentationen, frühere Kontakte, Empfehlungen und andere Aktivitäten zur Lead-Generierung aufgebaut. Die bestehenden 900 Kontakte werden in Sales Qualified Leads (SQLs) umgewandelt. Der Direktvertrieb nutzt seine Kontakte und SQLs, um Geschäfte abzuschließen. Im Channel-Vertrieb werden die Partnerschaften mit Beratern, Integratoren und Lieferanten ausgebaut.

PRIMARY TARGET
Threat Assessment, Automation & Response

Verfahren und Plattform zur Bestimmung von Gegenmaßnahmen gegen Sicherheitsprobleme und zum Schutz der Industrieobjekte

Technisches Gebiet

Die vorliegenden Forschungs- und Entwicklungsergebnisse beziehen sich allgemein auf das Gebiet der Cybersicherheit und der Systeme zur Bewertung von Sicherheitsrisiken, insbesondere auf ein Verfahren und eine Plattform zur Verringerung von Risiken, die durch Bedrohungen und Schwachstellen einer technischen Infrastruktur entstehen.

Technischer Hintergrund

Die Cybersicherheit von Industriegütern betrifft alle vorsätzlichen Angriffe auf das System mit dem Ziel, kritische Daten zu stehlen/manipulieren oder zu verfälschen oder durch Veränderung der Systemsteuerung erheblichen Schaden anzurichten, der für den Eigentümer des Industrieprodukts und das Umfeld, in dem es betrieben wird, mit erheblichen Problemen und Kosten verbunden ist. Jeder Hersteller ist bestrebt, die Risiken eines Cyber-Angriffs so weit wie möglich zu reduzieren, wobei Zeit und Kosten für Gegenmaßnahmen realistisch eingeschätzt werden müssen.

Industrielle Produkte sind heute zunehmend komplex und bestehen aus einfachen Bauteilen, Baugruppen, elektronischen Komponenten und Netzwerken. Diese Komponenten können Hardware und/oder Software für mindestens eine der Funktionen Datenverarbeitung, Datenübertragung, Datenmanagement usw. enthalten. Diese Komponenten von Datensystemen sind in der Regel Bedrohungen ausgesetzt und weisen bekannte Schwachstellen im Bereich der Cyber-Sicherheit auf.

Eine typische Sicherheitsinfrastruktur eines Unternehmens besteht aus verschiedenen Werkzeugen, die auf mehrere OSI-Schichten abzielen, z. B. Transport-, Daten-, Anwendungsnetzwerke und dergleichen. Diese Werkzeuge bieten ein allgemeines Schutzniveau, lassen aber bekannte Bedrohungen und Schwachstellen unbehandelt und können darüber hinaus durch die Werkzeuge selbst zusätzliche Bedrohungen und Schwachstellen einführen.

Darüber hinaus gibt es kein allgemeines Verfahren, mit dem ein Sicherheitsmanager angesichts begrenzter Zeit, Fähigkeiten, Arbeitskräfte und finanzieller Ressourcen entscheiden kann, welches Sicherheitsproblem als nächstes angegangen werden soll. Während Sicherheitsschwachstellen in Industrieprodukten in der Regel durch Software- oder Hardware-Patches behoben werden können, ist der Umgang mit Bedrohungen schwieriger, da die Art des Angriffs nicht immer vorhersehbar ist.

Die Risikobewertung wird ausführlich behandelt, z. B. in der WO 2012/109633 A2, einer Plattform zur Verwaltung von Sicherheitsgegenmaßnahmen, die es Benutzern von Sicherheits- und Compliance-Systemen ermöglicht, Risiken und Schwachstellen in ihrer Umgebung mit dem zusätzlichen Kontext zu betrachten, welche anderen abschwächenden Sicherheitsgegenmaßnahmen mit dieser Schwachstelle verbunden und innerhalb der gesamten Sicherheitsarchitektur anwendbar und/oder verfügbar sind. Darüber hinaus ermöglicht die Plattform den Nutzern, eine oder mehrere Maßnahmen zu ergreifen, die von der Steuerung des Betriebs einer Sicherheitsgegenmaßnahme zu Abschwächungszwecken bis hin zur einfachen Dokumentation des Bekanntheitsgrads einer bestehenden Sicherheitsgegenmaßnahme reichen.

Darüber hinaus offenbart das Dokument US 2014/0137257 A1 ein Verfahren zur Bewertung eines Risikos von einem oder mehreren Assets innerhalb einer betrieblichen Technologieinfrastruktur, das die folgenden Schritte umfasst: Bereitstellen einer Datenbank, die Daten enthält, die sich auf den einen oder die mehreren Assets beziehen, Berechnen einer Bedrohungsbewertung für den einen oder die mehreren Assets unter Verwendung eines oder mehrerer Prozessoren, die kommunikativ mit der Datenbank

verbunden sind, Berechnen einer Schwachstellenbewertung für den einen oder die mehreren Asset unter Verwendung des einen oder der mehreren Prozessoren, Berechnen einer Auswirkungsbewertung für den einen oder die mehreren Asset unter Verwendung des einen oder der mehreren Prozessoren; und Bestimmen des Risikos der einen oder mehreren Anlagen auf der Grundlage der Bedrohungsbewertung, der Schwachstellenbewertung und der Auswirkungsbewertung unter Verwendung des einen oder der mehreren Prozessoren.

Zusammenfassung der Erfindung

Die vorliegende Erfindung betrifft ein Verfahren zur Ermittlung von Gegenmaßnahmen gegen potentielle Bedrohungen eines Datensystems und eine entsprechende Plattform zur Ermittlung von Sicherheitsgegenmaßnahmen gemäß dem weiteren unabhängigen Anforderung.

Bevorzugte Ausführungsformen sind in den Anforderungen angegeben.

Mit der Softwarelösung werden Verfahren zur Auswahl von Gegenmaßnahmen für potentielle Bedrohungen von Assets eines Datensystems bereitgestellt, die die folgenden Schritte umfasst:

- Bereitstellen einer Konfiguration des Datensystems, einschließlich seines Assets, bestehend aus Geräten, Software, Daten, Datenübertragung und deren Verbindungen untereinander;
- Abrufen eines Satzes relevanter OSI-Schichten, auf denen bekannte Sicherheitsvektoren existieren können, aus einer Datenbank für jede Anlage, für jede abgerufene OSI-Schicht jeder Anlage, Abrufen von potenziellen Bedrohungen aus der Datenbank, die jeweils einem oder mehreren Sicherheitsattributen zugeordnet sind, die jeweils ein Ziel der Cybersicherheit definieren, wobei die potenziellen Bedrohungen einem oder mehreren Bedrohungsdurchführbarkeitsattributen zugeordnet sind, die jeweils einen Grad eines Durchführbarkeitsaspekts angeben, der ein durch die jeweilige potenzielle Bedrohung auferlegtes Sicherheitsrisiko ausgleicht;
- Verwenden der Datenbank, Zuordnen von mindestens einer Gegenmaßnahme aus einem Satz von Gegenmaßnahmen zu jeder der potenziellen Bedrohungen, wobei jede Gegenmaßnahme mindestens ein Gegenmaßnahme-Durchführbarkeitsattribut hat, das jeweils ein Niveau eines Durchführbarkeitsaspekts angibt, das erreicht wird, wenn die Gegenmaßnahme auf die potenzielle Bedrohung angewendet wird, wobei die Gegenmaßnahme geeignet ist, das Sicherheitsrisiko der jeweiligen potenziellen Bedrohung in einem oder mehreren Aspekten von Bedrohungs-Durchführbarkeitsattributen zu reduzieren;
- Automatisches Durchführen einer Optimierung, um eine oder mehrere Gegenmaßnahmen aus dem Satz von Gegenmaßnahmen auszuwählen, so dass die ausgewählten Gegenmaßnahmen ausreichen, um ein Gesamtsicherheitsrisiko unter ein gegebenes Niveau des Sicherheitsrisikos zu reduzieren.

Datensysteme in jeder IT-Infrastruktur bestehen aus einer Vielzahl von Assets. Ein Asset in einem Datensystem bezieht sich auf alles, das dem Datensystem hilft, seine Aufgaben und Ziele zu erfüllen. Zu den Assets können Hardware-Komponenten oder -Geräte wie Server, Speicherprozessoren und dergleichen, Software-Komponenten wie Datenbanken, Anwendungen und dergleichen, Daten wie Kundeninformationen, Finanzunterlagen usw., Datenübertragungen zwischen Assets und ein Netzwerk, das die Verbindung zwischen Hardware- und Software-Komponenten darstellt, gehören. Assets sind anfällig für Bedrohungen, die potenzielle Schadensquellen darstellen, wie z. B. Cyberangriffe, Systemausfälle oder menschliches Versagen.

Bedrohungen in einem Datensystem beziehen sich auf potenzielle Sicherheitsprobleme oder Gefahren, die die Sicherheit, Integrität und Verfügbarkeit des Datensystems beeinträchtigen könnten, wie z. B. unbefugter Zugriff, Manipulationen, Spoofing und Systemausfälle. Im Gegensatz dazu beziehen sich

Schwachstellen auf Schwachstellen in der Architektur, in der Implementierung oder in der Konfiguration des Systems, die von Angreifern ausgenutzt werden können, um Zugang zu sensiblen Informationen zu erhalten oder den normalen Systembetrieb zu stören. Beispiele für Schwachstellen sind ungepatchte Software, schwache Passwörter und offene Netzwerkports. Die Beseitigung sowohl von Bedrohungen als auch von Schwachstellen ist entscheidend für die Sicherheit und Zuverlässigkeit eines Industrieobjektes.

Das Ziel der Cybersicherheit ist der Schutz von Informationen und Systemen vor Cyberbedrohungen. Die Gegenmaßnahmen sind Mittel, um dieses Ziel zu erreichen.

Ein Datensystem setzt sich aus Assets zusammen. Jedes Asset ist mit einer oder mehreren Schichten des OSI-Modells (Open Systems Interconnection) oder eines ähnlichen Modells verbunden. Die Schichten definieren abstrakte Ebenen, auf denen der jeweilige Assets interagiert.

Die Schichten des OSI-Modells sind wie folgt:

1. Eine Übertragungschicht, die für die physikalische Übertragung von Daten zuständig ist und mit Anlagen, wie Netzwerkkabeln, Switches und Routern, verbunden ist,
2. eine Sicherungsschicht, die für die zuverlässige Übertragung von Datenrahmen zuständig ist und mit Anlagen wie Netzadaptern und Brücken verbunden ist,
3. eine Vermittlungsschicht, die für die Weiterleitung von Daten zuständig ist und mit Anlagen wie Routern und Gateways verbunden ist,
4. eine Transportschicht, die für die zuverlässige Übermittlung von Daten zuständig ist und zu den Anlagen gehört, wie z. B. Transportprotokolle, z. B. TCP, UDP, und Transportdienste,
5. eine Kommunikationsschicht, die für den Aufbau, die Aufrechterhaltung und die Beendigung von Kommunikationssitzungen zuständig ist und mit Anlagen wie Sitzungsprotokollen und Sitzungsverwaltungsdiensten verbunden ist,
6. eine Darstellungsschicht, die für die Formatierung und Verschlüsselung von Daten zuständig ist und zu den Anlagen gehört, z. B. Datenkomprimierung und Verschlüsselungsalgorithmen, und
7. eine Anwendungsschicht, die für die Dienste auf der Benutzerebene zuständig ist und mit Bestandteilen wie Anwendungsprotokollen, z. B. http, FTP usw. und Softwareanwendungen verbunden ist.

Jede dieser auf OSI-Schichten aufbauenden Assets kann für Bedrohungen anfällig sein, die potenziell ein oder mehrere Cybersicherheitsattribute betreffen, darunter bekannte Aspekte wie Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit des Datensystems. Diese Cybersicherheitsattribute definieren ein Cybersicherheitsziel und sollten für jede relevante OSI-Schicht jedes Assets des zu sichernden Datensystems gewährleistet werden.

Die Integrität bezieht sich auf die Genauigkeit und Konsistenz der Daten während ihrer gesamten Lebensdauer, d. h. es muss sichergestellt werden, dass die Daten nicht auf unbefugte Weise verändert oder verfälscht werden. Vertraulichkeit bezieht sich auf den Schutz sensibler Informationen vor unbefugter Offenlegung, und Verfügbarkeit bezieht sich auf die Zugänglichkeit von Daten auf Anfrage.

Es wird eine Bedrohungsdatenbank zur Verfügung gestellt, die so konfiguriert ist, dass sie Assets jeder Art von Infrastruktur mit den beteiligten OSI-Schichten und jede OSI-Schicht der jeweiligen Assets mit einer oder mehreren potenziellen Bedrohungen verknüpft. Jede Bedrohung ist für mindestens einen der Aspekte der Cybersicherheitsattribute relevant.

Bei einer bestimmten Konfiguration des zu sichernden Datensystems, die durch seine Assets und deren Verbindungen definiert ist, kann für jedes Assets ein Satz relevanter OSI-Schichten aus der Datenbank abgerufen werden, wobei ferner für jede identifizierte OSI-Schicht der Assets eine oder mehrere

potenzielle Bedrohungen aus der Datenbank abgerufen werden. Jede Bedrohung betrifft ein oder mehrere Cybersicherheitsattribute (Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit) auf eine bestimmte Weise.

Darüber hinaus enthält die Datenbank Informationen über den Schweregrad der Bedrohungen in Bezug auf ihre Durchführbarkeit, d. h. die Schwierigkeit, die potenzielle Bedrohung zu nutzen. Die Durchführbarkeit wird durch Attribute zur Durchführbarkeit der Bedrohung angegeben.

Das Attribut „Durchführbarkeit der Bedrohung“ bezieht sich auf die Wahrscheinlichkeit, dass die Bedrohung tatsächlich erfolgreich ausgeführt werden und dem zugehörigen Asset des Datensystems Schaden zufügen oder eines der Cybersicherheitsattribute in Bezug auf den jeweiligen Asset beeinträchtigen könnte. Das Attribut Durchführbarkeit berücksichtigt Aspekte der Durchführbarkeit wie die Fähigkeiten des Angreifers, die Verfügbarkeit von Werkzeugen und Ressourcen, den bereits vorhandenen Schutz zur Eindämmung der Bedrohung und die Motivationen sowie die zur Abwehr der Bedrohung vorhandenen Sicherheitsmaßnahmen.

Darüber hinaus kann das Attribut/die Eigenschaft „Durchführbarkeit der Bedrohung“ nach Aspekten wie Angriffsvektor, Komplexität, Privilegien, Benutzerinteraktion, Reproduzierbarkeit, Komponenten, Wahrscheinlichkeit und dergleichen kategorisiert werden. „Expertise“ bedeutet das technische Wissen, das erforderlich ist, um die Bedrohung für einen Angriff zu nutzen, ‚Angriffsvektor‘ bedeutet die Komplexität des Angriffs, bei dem die Bedrohung erfolgreich genutzt wird, ‚Komplexität‘ gibt die Komplexität der Bedrohung an, ‚Privilegien‘ sind die Privilegien, die erforderlich sind, um Maßnahmen auszuführen, die eine Bedrohung darstellen, „Benutzerinteraktion“ gibt an, wie viel Interaktion erforderlich ist, um Maßnahmen auszuführen, die eine Bedrohung darstellen, ‚Reproduzierbarkeit‘ gibt die Schwierigkeit an, die Maßnahmen einer einmal entdeckten Bedrohung/Schwachstelle zu reproduzieren, ‚Komponenten‘ gibt den Grad der Komplexität der Komponenten an, die zur Durchführung des Angriffs erforderlich ist, und ‚Wahrscheinlichkeit‘ gibt die Wahrscheinlichkeit an, dass ein Angriff oder eine Bedrohung erfolgreich ist. Jeder Aspekt der Attribute für die Durchführbarkeit von Bedrohungen kann mit einem Wert bewertet werden, z. B. niedrig, mittel, hoch oder ähnlich, oder mit einem Wert zwischen 0 und 1, wobei 0 keine und 1 hohe Relevanz bedeutet.

Die Attribute zur Durchführbarkeit von Bedrohungen können für das Risikomanagement verwendet werden, um den Grad des Risikos zu bestimmen, das die Bedrohungen für die zugehörigen Assets darstellen. Bedrohungen mit einer höheren Ausprägung eines Aspekts eines Attributs zur Durchführbarkeit von Bedrohungen werden als höheres Risiko eingestuft und können bei der Planung von Schutzmaßnahmen und Reaktionen vorrangig behandelt werden. Bedrohungen mit einer niedrigeren Ausprägung eines Aspekts des Attributs „Durchführbarkeit der Bedrohung“ können eine niedrigere Priorität erhalten, da die Wahrscheinlichkeit, dass die Bedrohung ausgenutzt wird, gering ist.

Bei den Durchführbarkeitsattributen der Bedrohungen handelt es sich um dynamische Attribute, die auch von bereits im Datensystem getroffenen Gegenmaßnahmen abhängen oder diesen entgegenwirken können. Das Gesamtsicherheitsrisiko in einem Datensystem hängt von den Stufen jeder potenziellen Bedrohung und ihren Durchführbarkeitsattributen ab, die für jede relevante OSI-Schicht jedes zum Datensystem gehörenden Objekts ermittelt wurden. Das Gesamtsicherheitsrisiko des Datensystems, das z. B. in Form einer Gesamtsicherheitsmetrik angegeben wird, kann also durch die Konjunktion der Stufen jedes Bedrohungsdurchführbarkeitsattributs jeder bestehenden Bedrohung und insbesondere durch die Stufe jedes von der jeweiligen Bedrohung betroffenen Cybersicherheitsattributs bewertet werden.

Der Begriff „Gegenmaßnahme“ bezieht sich auf eine Sicherheitslösung, die dazu dient, eine bestimmte Bedrohung zu bekämpfen, die von einer Anlage des Datensystems ausgeht. In der Regel wird eine

Gegenmaßnahme auf einer oder mehreren OSI-Schichten in Bezug auf ein bestimmtes Gut eingesetzt, so dass Gegenmaßnahmen die Implementierung einer Firewall, den Schutz von Datenverbindungen, die Installation von Überwachungssoftware und Ähnliches umfassen können. Eine Gegenmaßnahme wird als ein Asset betrachtet, das auch auf der OSI-Schicht zu finden ist, wie z. B. ein (HSM) Hardware-Sicherheitsmodul, das auch neue Angriffsvektoren für potenzielle Bedrohungen des Systems hinzufügen kann. Zu den Gegenmaßnahmen gehören unter anderem netzbasierte IDS/IPS, hostbasierte IDS/IPS, sichere E-Mail-Gateways, sichere Web-Gateways, integrierte Sicherheitsanwendungen, Web Application Firewalls, Netzzugangskontrolle, Plattformen zum Schutz von Endpunkten, Lösungen für virtuelle private Netze, Switches, Router, Lösungen für die Anwendungskontrolle, Lösungen zur Verhinderung von Datenverlusten (DLP), Lösungen für den verwalteten Dateitransfer, Überwachung der Dateiintegrität, E-Mail-Verschlüsselung, Datenbankverschlüsselung sowie Anwendungshärtung und -abschirmung.

Gegenmaßnahmen, die zur Abschwächung oder Beseitigung der Bedrohungen eingesetzt werden können, verringern daher potenziell das Gesamtsicherheitsrisiko (angegeben durch die Gesamtsicherheitsmetrik), das das Datensystem darstellt. Jede auf eine potenzielle Bedrohung gerichtete Gegenmaßnahme kann sich auf mindestens eines der mit der jeweiligen Bedrohung verbundenen Attribute der Durchführbarkeit der Bedrohung auswirken. Darüber hinaus kann sich jede angewandte Gegenmaßnahme auf einen oder mehrere Aspekte des Attributs „Durchführbarkeit der Bedrohung“ auswirken, da die Gegenmaßnahme die Durchführung der Bedrohung unmöglich macht oder den Aufwand für einen oder mehrere der oben genannten Aspekte des Attributs „Durchführbarkeit der Bedrohung“ erhöht.

Daher werden die den Bedrohungen zugeordneten Gegenmaßnahmen mit einem entsprechenden Attribut für die Durchführbarkeit der Gegenmaßnahme verknüpft, das ein Niveau oder einen Wert für jeden Aspekt der Durchführbarkeit angibt, der erreicht wird, wenn die entsprechende Gegenmaßnahme angewendet wird. Daher kann die Datenbank die Bewertung jeder Gegenmaßnahme im Hinblick auf ihre Wirksamkeit bei der Abschwächung oder Beseitigung der entsprechenden potenziellen Bedrohung ermöglichen.

Mit anderen Worten, jede angewendete Gegenmaßnahme kann ein Durchführbarkeitsattribut für die Gegenmaßnahme haben, das sich bei Anwendung auf ein oder mehrere Durchführbarkeitsattribute der Bedrohung auswirkt, für die die Gegenmaßnahme ausgewählt wurde. Das Attribut „Durchführbarkeit der Gegenmaßnahme“ kann daher die Wahrscheinlichkeit eines erfolgreichen Angriffs verringern, z. B. dadurch, dass ein Angreifer mehr Fachwissen benötigt und/oder der Angriffsvektor komplexer sein muss, was zu einer längeren Dauer für die Durchführung des Angriffs führen kann und den Angreifer möglicherweise daran hindert, die potenzielle Bedrohung zu nutzen.

Das Gesamtsicherheitsrisiko kann mittels einer Gesamtsicherheitsmetrik bewertet werden, die auf der Grundlage der Bedrohungsdurchführbarkeitsattribute aller potenziellen Bedrohungen und des Gegenmaßnahmen-Durchführbarkeitsattributs aller in Betracht gezogenen Gegenmaßnahmen berechnet wird, wobei die Optimierung auf der Grundlage einer Minimierung einer Kostenfunktion durchgeführt wird, die von der Gesamtsicherheitsmetrik abhängt. Die Gesamtsicherheitsmetrik kann durch Gewichtung der Durchführbarkeitsstufen berechnet werden.

Nach dem obigen Verfahren soll ein Risikomanagement durchgeführt werden mit dem Ziel, die wirksamsten Gegenmaßnahmen oder eine wirksame Reihenfolge von Gegenmaßnahmen zu bestimmen, die anzuwenden sind, um Sicherheitsrisiken des zu sichernden Datensystems zu reduzieren. Es hat sich gezeigt, dass die Anwendung von Gegenmaßnahmen, die den größten Einfluss (Minderung oder Beseitigung des durch die Bedrohungen implizierten Risikos) auf die Durchführbarkeitsattribute der identifizierten Bedrohungen (die von den jeweiligen Gegenmaßnahmen betroffen sind) für ein Datensystem haben, nicht unbedingt zum bestmöglichen Ergebnis in Bezug auf die Risikominderung führt.

Darüber hinaus kann die Kostenfunktion der Optimierung von den Ressourcen abhängen, die für die Umsetzung der jeweils betrachteten Gegenmaßnahmen benötigt werden, insbesondere von Zeit, Material, Budget, Arbeitskräften, Fähigkeiten, Verarbeitungs- und Speicherkapazität.

Zu berücksichtigen sind auch die zusätzlichen potenziellen Bedrohungen, die durch die Umsetzung/Anwendung einer oder mehrerer der ermittelten Gegenmaßnahmen hinzukommen und im schlimmsten Fall zu einem erhöhten Gesamtsicherheitsrisiko führen können (Gesamtsicherheitskennzahl). Daher ist der Prozess der Bestimmung der effektivsten Gegenmaßnahmen nicht trivial, und es hat sich gezeigt, dass eine Optimierung zu einer optimierten Auswahl eines Satzes von Gegenmaßnahmen führen kann, die mit bestimmten begrenzten Ressourcen wie Zeit, Kosten, Arbeitskräften, Fähigkeiten und dergleichen angewendet werden können, oder zu einer Reihenfolge der anzuwendenden Gegenmaßnahmen, um den bestmöglichen Anstieg der Gesamtsicherheitsmetrik zu erzielen, oder zu einer Liste mit Gegenmaßnahmen in der Reihenfolge des Sicherheitsgewinns bei deren Anwendung.

Nach dem obigen Verfahren kann eine Optimierung durchgeführt werden, indem die Auswirkungen jeder Gegenmaßnahme in Bezug auf die Verringerung des Gesamtsicherheitsrisikos bewertet werden.

Es kann vorgesehen werden, dass die ausgewählten Gegenmaßnahmen nacheinander bestimmt werden, indem iterativ Optimierungsschritte jeweils nach der Annahme der Anwendung der zuvor ausgewählten Gegenmaßnahmen durchgeführt werden.

Insbesondere umfasst die Annahme der Anwendung der zuvor ausgewählten Gegenmaßnahmen das Hinzufügen eines oder mehrerer weiterer Assets, die durch die angenommene Anwendung der Gegenmaßnahme verursacht werden, wobei dem einen oder den mehreren weiteren Assets mindestens eine neue Bedrohung und mindestens eine neue Gegenmaßnahme zugeordnet ist, wobei die nächste Iteration der Optimierung die mindestens eine neue Bedrohung und mindestens eine neue Gegenmaßnahme berücksichtigt.

Insbesondere kann bei der Annahme der Anwendung der zuvor ausgewählten Gegenmaßnahmen ein weiterer Asset, der durch die angenommene Anwendung der Gegenmaßnahme verursacht wird, berücksichtigt werden, dem mindestens eine angenommene Bedrohung zugeordnet ist, wobei die nächste Iteration der Optimierung die mindestens eine angenommene Bedrohung berücksichtigt.

So kann auch die Erhöhung des Sicherheitsrisikos durch die Anwendung der Gegenmaßnahme berücksichtigt werden. Bei der Optimierung der Auswahl oder der Reihenfolge von Gegenmaßnahmen führen daher Gegenmaßnahmen gegen Bedrohungen, die auch zusätzliche Werte darstellen, selbst zu Bedrohungen. Daher kann die Optimierung in einer oder mehreren Iterationen durchgeführt werden, wenn neue Bedrohungen durch die angenommene Anwendung von Gegenmaßnahmen eingeführt werden. Als Ergebnis der Optimierung können die verfügbaren Ressourcen weiter berücksichtigt werden, um die Anzahl oder den Umfang der anzuwendenden Gegenmaßnahmen zu begrenzen.

Bei der Optimierungsmethode kann ein logischer Algorithmus verwendet werden, der versucht, die wirksamste(n) Gegenmaßnahme(n) zu finden.

Der Vorteil der Optimierung besteht im Wesentlichen darin, eine oder mehrere Gegenmaßnahmen zu finden, die das gesamte Sicherheitsrisiko oder zumindest ein potenzielles Risiko verringern können. So können vorzugsweise Gegenmaßnahmen gefunden werden, die mehrere Risiken auf einmal reduzieren, auch auf mehr als einer OSI-Schicht.

Die Optimierung kann anhand einer Kostenfunktion erfolgen, die von den für die Umsetzung jeder Gegenmaßnahme verfügbaren Ressourcen abhängt.

Die ausgewählten Gegenmaßnahmen können sukzessive bestimmt werden, indem iterativ Optimierungsschritte durchgeführt werden, wobei in jeder Iteration die Anwendung der zuvor ausgewählten Gegenmaßnahmen angenommen wird.

Es kann vorgesehen werden, dass die ermittelten Gegenmaßnahmen durch einen Gegenmaßnahmenmechanismus angewandt werden, um die Sicherheitslücken durch die Durchführung der einen oder mehreren ermittelten Gegenmaßnahmen zu schließen. Bei dem Gegenmaßnahmenmechanismus kann es sich um einen der folgenden Mechanismen handeln: ein netzwerkbasiertes IDS/IPS, ein hostbasiertes IDS/IPS, ein sicheres E-Mail-Gateway, ein sicheres Web-Gateway, eine integrierte Sicherheitsanwendung, eine Webanwendungs-Firewall, eine Netzwerkzugangskontrolle, eine Endpunktschutzplattform, ein virtuelles privates Netzwerk, einen Switch, einen Router, eine Anwendungskontrollvorrichtung, eine Vorrichtung zur Verhinderung von Datenverlusten (DLP), eine verwaltete Dateiübertragungsvorrichtung, eine Dateiintegritätsüberwachung, eine E-Mail-Verschlüsselungsvorrichtung, eine Datenbankverschlüsselungsvorrichtung und eine Vorrichtung zur Anwendungshärtung und -abschirmung.

Der Mechanismus für Gegenmaßnahmen kann eine Strategie für den Einsatz von Gegenmaßnahmen bereitstellen, um die festgelegten Gegenmaßnahmen in der vorgegebenen Reihenfolge bereitzustellen.

Kurzbeschreibung der Zeichnungen

Ausführungsformen werden in Verbindung mit den beigefügten Zeichnungen näher beschrieben:

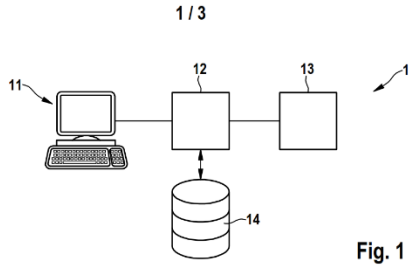

Fig. 1

Fig. 1 zeigt schematisch ein Computersystem, das eine Plattform für das Risikomanagement darstellt;

Fig. 1 zeigt schematisch eine Plattform 1 zur Ermittlung von Gegenmaßnahmen zur Verringerung des Sicherheitsrisikos eines Industrieproduktes. Die Plattform 1 kann auf einer herkömmlichen Computer-umgebung ausgeführt werden, die eine Reihe von Einheiten umfassen kann, wie z.B. eine Benutzer-schnittstelle 11, die z.B. eine Tastatur, eine Maus, eine Anzeige und dergleichen umfasst, um einem Benutzer die Interaktion mit einem oder mehreren Aspekten der Plattform zu ermöglichen, eine Verarbeitungseinheit 12 zur Durchführung des Verfahrens zur Auswahl geeigneter Gegenmaßnahmen zur Verringerung des Gesamtsicherheitsrisikos eines gegebenen Industrieproduktes und einen Speicher 13 zur Speicherung von Programmcode für den Algorithmus zur Auswahl von Gegenmaßnahmen, Konfigurations-daten, Benutzerdaten und dergleichen.

Grundsätzlich wird die Plattform von Fig. 1 verwendet, um das Gesamtsicherheitsrisiko einer gegebenen Konfiguration eines Datensystems zu analysieren und geeignete Gegenmaßnahmen auszuwählen, die mit optimierter Effizienz angewendet werden. Die Plattform 1 kann eine Datenbank enthalten oder in Datenkommunikation mit einer entfernten Datenbank 14 (Cloud) stehen. Ein Mechanismus für Gegenmaßnahmen kann in der Verarbeitungseinheit 12 angewendet werden.

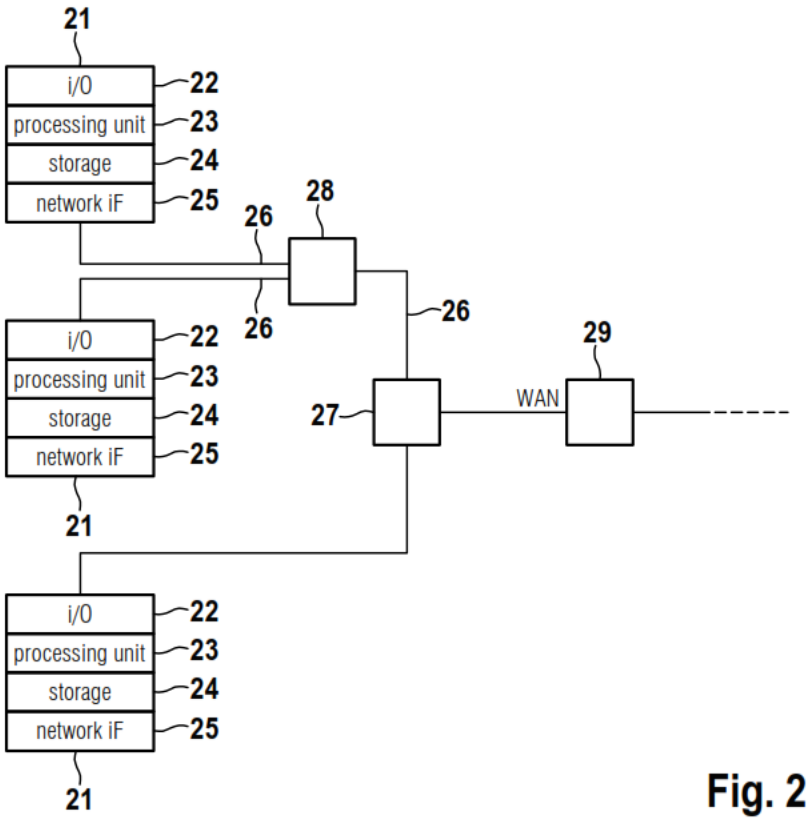

Fig. 2

Fig. 2 zeigt schematisch ein beispielhaftes, zu sicherndes Datensystem;

Ein Beispiel für ein zu sicherndes Datensystem ist in Fig. 2 dargestellt. Das Datensystem 2 von Fig. 2 umfasst eine Reihe von Terminals 21, die jeweils ein Eingabe-Ausgabe-Mittel 22, wie z. B. eine Tastatur und einen Bildschirm, eine Verarbeitungseinheit 23, einen Speicher 24 und Netzwerkschnittstellen 25 aufweisen. Die Terminals 21 sind über drahtgebundene Netzwerkverbindungen 26 zur Kommunikation über TCP unter Verwendung eines Routers 27 und Switches 28 miteinander verbunden, wobei der Router über eine Hardware-Firewall 29 mit einem Wide Area Network (WAN) verbunden ist. Jedes der Endgeräte 21 kann eine oder mehrere Software-Instanzen ausführen. Bei dem hier beispielhaft beschriebenen Datensystem 2 kann es sich um ein Standard-Firmennetz für kleine oder mittlere Unternehmen handeln.

Ein solches Client-Server-Datensystem 2, wie es in Fig. 2 dargestellt ist, ist offen für verschiedene Sicherheitsbedrohungen, die die Funktionsfähigkeit sowie die Vertraulichkeit, Integrität und Verfügbarkeit des Datensystems beeinträchtigen können.

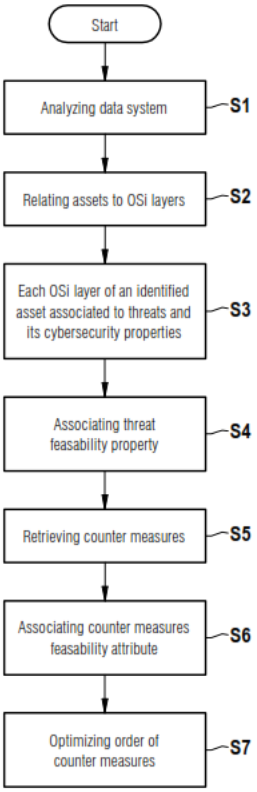

Fig. 3

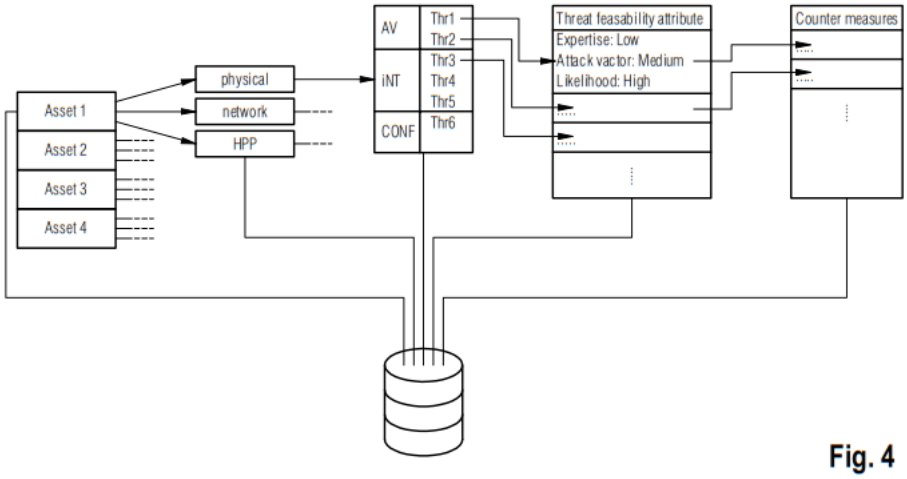

Fig. 4

Abb. 4 zeigt eine schematische Darstellung einer Datenbank zum Abrufen von Gegenmaßnahmen.

Fig. 3 zeigt ein Flussdiagramm zur Veranschaulichung des Verfahrens zur Bestimmung von Sicherheitsgegenmaßnahmen in einem gegebenen Datensystem eines Industrieobjektes;

Vorgehensweise zum Abruf von Gegenmaßnahmen

In Verbindung mit dem Flussdiagramm in Fig. 3 wird ein Verfahren zur Analyse der Daten und zur Bestimmung geeigneter Sicherheitsmaßnahmen beschrieben. Darüber hinaus veranschaulicht Fig. 4 die Interaktion mit Informationen aus der Datenbank.

Schritt S1

In **Schritt S1** wird das Datensystem 2 auf seine Assets hin analysiert. Die Assets werden durch Analyse der verwendeten Komponenten 21-29, der implementierten Protokolle, der installierten Software und dergleichen identifiziert. Es wird eine Liste der Assets (Asset1, Asset2, ...) des Datensystems erstellt. Jede Anlage kann eine oder mehrere Schichten haben, wie Hardware, Software, Daten, Signale und dergleichen. Jedes Asset hat seine eigenen Anforderungen in Bezug auf Sicherheitsaspekte, die durch Cybersicherheitsattribute gegeben sind, einschließlich Aspekten wie Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit des Datensystems.

Schritt S2

In **Schritt S2** werden die Assets durch Abfrage der Datenbank 14 mit ihren jeweiligen OSI-Schichten (physische, Datenverbindungs-, Netzwerk-, Transport-, Kommunikations-, Präsentations- und Anwendungsschicht) in Beziehung gesetzt, so dass eine Liste spezifischer Assets, die zum Datensystem gehören, entsteht.

Die OSI-Schicht beschreibt die Trennung von Inhalten, aber jedes Asset kann sich auf mehrere Schichten stützen

Asset	OSI Schicht(en)
DATA	Virtuell
FTP	Schicht 7 – Anwendungsschicht
TCP	Schicht 4 – Transportschicht
IP	Schicht 3 – Vermittlungsschicht
IEEE 802.3	Schicht 2 – Datenübertragungsschicht
IEE 802.3x Gigabit Ethernet Kabel	Schicht 1 – Bitübertragungsschicht
Tastatur	Schicht 1 – Bitübertragungsschicht
Software	Schicht 7 – Anwendungsschicht
Netzwerkschnittstelle	Schicht 1 – Bitübertragungsschicht
Netzwerkschnittstelle	Schicht 2 – Datenübertragungsschicht

Die Tabelle zeigt die Zuordnung einiger Assets des Datensystems 2 zu den beteiligten OSI-Schichten als Ergebnis von Schritt S2.

Die Zuordnung zu einer OSI-Schicht ist wichtig, da hierdurch Bedrohungen über die der OSI-Schicht zugeordneten Sicherheitseigenschaften mit Werten abgeglichen werden können. Daher bestimmen die Werte die Sicherheitseigenschaften im Hinblick auf den erforderlichen Schutz.

Im Allgemeinen haben Assets jeweils ihre eigenen Anforderungen an die Sicherheit, d.h. Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit. Bedrohungen werden mit Hilfe dieser Eigenschaften auf die Werte abgebildet. Alle Werte, Bedrohungen und Gegenmaßnahmen sind mit einer oder mehreren OSI-Schichten verbunden. Daher ist die Verbindung zwischen Assets und Bedrohungen durch die OSI-Schicht und die Cybersicherheitseigenschaften gegeben. Ein Beispiel: FTP ist ein Protokoll und gehört zur Anwendungsschicht des OSI-Modells. FTP ist auch ein Protokoll, das auf TCP/IP basiert, das Teil des Ethernet-Protokolls ist. Wenn FTP Teil einer Anlage ist, sind die OSI-Schichten Anwendungsschicht (7), Transportschicht (4), Vermittlungsschicht (3), Datenübertragungsschicht (2) und Bitübertragungsschicht (1) betroffen. Jeder der Schichten werden Bedrohungen als Angriffsvektor zugeordnet, die eine oder alle ihrer Sicherheitseigenschaften (Vertraulichkeit, Verfügbarkeit oder Integrität) verletzen. Wenn die Verfügbarkeit von FTP angegriffen werden soll, können die Bedrohungen für jede der Schichten bestimmt werden, z. B. DDOS-Angriff auf Schicht 4, MAC-Spoofing auf Schicht 3, Durchtrennen von Kabeln auf Schicht 1.

Schritt S3

Darüber hinaus wird die Datenbank 14 in **Schritt S3** abgefragt, um potenzielle Bedrohungen des Datensystems für jede der relevanten OSI-Schichten jedes der identifizierten Assets zu ermitteln. Die Bedrohungen werden anhand der OSI-Schichten und der relevanten Cybersicherheitseigenschaften auf die Anlagen abgebildet. Darüber hinaus klassifiziert die Datenbank 14 jede identifizierte Bedrohung mit Cybersicherheitsattributen, z. B. in Bezug auf Integrität, Verfügbarkeit und Vertraulichkeit. Beispiele für potenzielle Bedrohungen sind in der nachstehenden Tabelle aufgeführt:

Asset, OSI Schicht	**Bedrohung**
DATA	Veränderung der Daten (Integrität)
DATA / FTP	DATA / FTP Auslesen der Daten (Vertraulichkeit)

DATA / FTP	DDOS (Verfügbarkeit)
Kommunikation / Data Link	ARP Spoofing (Integrität)
Kommunikation / Data Link	MAC Address Spoofing (Vertraulichkeit, Integrität)
Kommunikation / Data Link	DDOS (Verfügbarkeit)

In einem Beispiel wird FTP in dem Datensystem 2 verwendet und bildet daher einen Asset. FTP ist ein Datenübertragungsprotokoll, das der Anwendungsschicht des OSI-Modells zugeordnet ist und auf TCP/IP basiert, das Teil des Ethernet-Protokolls ist, das der Transportschicht, der Netzwerkschicht, der Datenverbindungsschicht und der physikalischen Schicht des OSI-Modells zugeordnet ist.

Für jede dieser Schichten werden die Bedrohungen durch Abfrage der Datenbank auf der Grundlage des Angriffsvektors ermittelt. Wenn es um die Verfügbarkeit geht, können die Bedrohungen anhand der zugehörigen Schichten des OSI-Modells ermittelt werden. In Bezug auf die Verfügbarkeit von FTP-Angriffen kann ein DDOS-Angriff auf der Transportschicht, ein MAC-Spoofing auf der Netzwerkschicht 3, ein Schnittkabelangriff auf der physikalischen Schicht möglich sein.

Schritt S4

In **Schritt S4** wird jede identifizierte Bedrohung mit einem Attribut für die Durchführbarkeit der Bedrohung verknüpft, das nach Aspekten wie Angriffsvektor, Komplexität, Privilegien, Benutzerinteraktion, Reproduzierbarkeit, Ausrüstung und Wahrscheinlichkeit kategorisiert wird, wie oben definiert

Jeder der Aspekte der Attribute zur Durchführbarkeit der Bedrohung wird mit einer Stufe kategorisiert oder mit Klassen wie „niedrig“, „mittel“ und „hoch“ oder als Werte wie 1 bis 5, 1 bis 100 oder Ähnliches bewertet.

Insbesondere können die Attribute zur Durchführbarkeit von Bedrohungen wie folgt kategorisiert werden:

Angriffsvektor	Netzwerk (5) , Benachbart (4), Lokales Netzwerk (3), Physisch (2) , Lokaler Computer (1)
Komplexität	Sehr einfach (1-100), Mittlere Komplexität(1-100), Sehr komplex(1-100))
Privilegien	Jeder (3) , Authentifiziert (2) , Root (1)
Benutzerinteraktion	Einfacher Aufwand(1-100), Mittlerer Aufwand(1-100), Zeitaufwendig(1-100), Mehrere Experten(1-100) erforderlich)
Reproduzierbarkeit	Leicht reproduzierbar (3), Schwer reproduzierbar (1), Muss neu bewertet werden (2)
Für den Angriff benötigte Ausrüstung	Standardausrüstung (3), Expertenausrüstung (2), Professionelle Ausrüstung (1)
Eintrittswahrscheinlichkeit	Sehr wahrscheinlich (3), Wahrscheinlich (2), Unwahrscheinlich (1)

Jede der Kategorien ist mit einer Zahl kodiert. Die Kategorien können eine höhere Zahl haben, je höher die Wahrscheinlichkeit eines erfolgreichen Angriffs auf der Grundlage des Attributs der Durchführbarkeit der Bedrohung ist.

Zum Beispiel können Bedrohungen wie Man in the Middle und DDOS wie folgt kategorisiert werden:

Bedrohung	**Bedrohungsmerkmal Machbarkeit**
Man in The Middle zum Auslesen von Daten,	Angriffsvektor für Vertraulichkeit: Lokales Netzwerk (3) Komplexität: Sehr einfach (50) Privilegien: Jeder (3) Benutzer-Interaktion: Einfacher Aufwand (60) Reproduzierbarkeit: Leicht reproduzierbar (3) Ausstattung: Standard (1) Eintrittswahrscheinlichkeit: Sehr Wahrscheinlich (3)
DDOS Angriff, Verfügbarkeit	Lokales Netzwerk (3) Komplexität: Sehr einfach (80) Privilegien: Jeder (3) Benutzer-Interaktion: Einfacher Aufwand (90) Reproduzierbarkeit: Leicht reproduzierbar (3) Ausstattung: Standard (3) Eintrittswahrscheinlichkeit: Sehr Wahrscheinlich (3)

Schritt S5

Durch Abfrage der Datenbank 14 zu jeder der Bedrohungen werden in **Schritt S5** eine oder mehrere Gegenmaßnahmen definiert. Die Datenbank 14 assoziiert einfach mögliche Gegenmaßnahmen für zumindest einige der potenziellen Bedrohungen und jedes jeweils betroffene Cybersicherheitsattribut. Als Ergebnis erhält man eine Liste von Gegenmaßnahmen, die eine Wirkung auf die vom Datensystem implizierten Bedrohungen haben.

Schritt S6

Darüber hinaus wird jede erhaltene Gegenmaßnahme in **Schritt S6** mit einem Durchführbarkeitsattribut für die Gegenmaßnahme verknüpft, das dieselben Aspekte wie das Durchführbarkeitsattribut für die Bedrohung aufweist, nämlich Angriffsvektor, Komplexität, Privilegien, Benutzerinteraktion, Reproduzierbarkeit, Ausrüstung und Eintrittswahrscheinlichkeit. Die entsprechenden Durchführbarkeitsattribute für Gegenmaßnahmen geben die Wirkung einer Gegenmaßnahme auf die Durchführbarkeitsattribute einer oder mehrerer spezifischer Bedrohungen an, wenn die Gegenmaßnahme gegen eine oder mehrere der identifizierten Bedrohungen angewendet wurde. Insbesondere in Bezug auf das Attribut der Durchführbarkeit der Gegenmaßnahme wird das Attribut der Durchführbarkeit der Bedrohung auf das Attribut der Durchführbarkeit der Gegenmaßnahme reduziert, wenn es kleiner ist.

Wenn Gegenmaßnahmen angewendet werden, kann die Gesamtsicherheit des Datensystems beeinflusst, vorzugsweise verbessert werden. Die Gesamtsicherheitsmetrik kann ein Durchschnitt aller Attribute für die

Durchführbarkeit von Bedrohungen sein, nachdem alle identifizierten Gegenmaßnahmen angewendet wurden. Um die Auswirkung von Gegenmaßnahmen auf die Gesamtsicherheit des Datensystems zu bewerten, wird die Änderung einer Gesamtsicherheitsmetrik durch die Anwendung der Gegenmaßnahmen berechnet. Daher können die Durchführbarkeitsattribute für Gegenmaßnahmen verwendet werden, um die kategorisierten Stufen oder Werte der Aspekte der Durchführbarkeitsattribute für Bedrohungen durch Anwendung einer Minimumfunktion zu verringern. Stufen können mit Werten in Beziehung gesetzt werden, so dass durch die Berechnung einer gewichteten Summe der Werte der Aspekte aller Bedrohungsdurchführbarkeitsattribute aller Bedrohungen eine Gesamtsicherheitsangabe, d. h. eine Effizienz der Maßnahmen, erhalten werden kann.

Die Effizienz wird als Differenz zwischen dem Wert der Aspekte des Attributs „Durchführbarkeit der Bedrohung“ vor Anwendung der Gegenmaßnahmen und nach Anwendung der Gegenmaßnahmen berechnet, z. B. in einer gewichteten Summe der Aspektwerte.

Eine Bedrohung und eine Gegenmaßnahme können sieben Durchführbarkeitsattribute für die Bedrohung und die Gegenmaßnahme haben (z. B. Angriffsvektor, Komplexität, Berechtigungen, Benutzerinteraktion, Reproduzierbarkeit, Ausrüstung und Wahrscheinlichkeit).

Außerdem ist eine Zielerreichbarkeit gegeben, die das Ziel des Prozesses zur Bestimmung von Gegenmaßnahmen definiert.

In einem Bedrohungsdurchführbarkeitsvektor V:= [e1, e2, e3, e4, e5, e6, e7]^T, der jeder möglichen Bedrohung zugeordnet ist, kann jedes Element als Angriffsvektor e1, Komplexität e2, Privilegien e3, Benutzerinteraktion e4, Reproduzierbarkeit e5, Ausrüstung e6 und Wahrscheinlichkeit e7 definiert werden. Der Vektorraum von V kann für eine beliebige Anzahl von Attributen zur Durchführbarkeit von Bedrohungen erweitert werden.

Ferner sei T ⊆ V die Menge aller identifizierten potentiellen Bedrohungen T={t1, t2, ..., tn} des analysierten Datensystems 2 und C ⊆ V die Menge aller Gegenmaßnahmen C={c1, c2, ..., ck}, die mit den identifizierten potentiellen Bedrohungen verbunden sind.

Um den Ist-Zustand unseres Systems darzustellen und die Wirkung aller eingesetzten Gegenmaßnahmen {c1, c2, ..., ck} zu erfassen, wird zunächst die Funktion M verwendet

$$M : T \times \prod_{i=1}^{k} C \to V$$

$$(t, c) \mapsto M((t, c)) := \sum_{i=1}^{7} \min\{t_i, (c_1)_i, (c_2)_i, ..., (c_k)_i\} e_i$$

wobei k ∈ N die Anzahl der verwendeten Gegenmaßnahmen C ist. Hinweis: Wenn eine Gegenmaßnahme keine Wirkung auf eine Bedrohungseigenschaft hat, kann die Koordinate auf ∞ oder auf den höchsten Wert auf unserer Skala der Bedrohungseigenschaften gesetzt werden. Aufgrund dieser Einstellung oder Auswahl hat die Gegenmaßnahme in der Berechnung ebenfalls null Wirkung.

Außerdem wird zur Berechnung der tatsächlichen Durchführbarkeit die Funktion $\mathfrak{F}$ verwendet. Um die Anzahl der früheren Bedrohungen eines Angriffspfades zu berücksichtigen, wird die Wahrscheinlichkeitskoordinate für jede betrachtete frühere Bedrohung T={t1, t2, ..., tk} um λ reduziert. λ ist ein Gewichtungsfaktor, der auf λ = 0,5 gesetzt werden kann, aber auch andere Werte sind möglich. Die Funktion $\mathfrak{F}$ ist definiert durch:

$$\mathfrak{F} : V \to \mathbb{R}$$

$$x \mapsto \mathfrak{F}(x) := \frac{< a, x - n\lambda e_7 >}{\sum\limits_{i=1}^{\dim V} < a_i, \mathbb{1} >} = \frac{\sum\limits_{i=1}^{\dim V} a_i x_i - n\lambda a_7}{\sum\limits_{i=1}^{\dim V} a_i}$$

wobei x ein allgemeiner Sicherheitsmaßstab und n ∈ N die Anzahl der zuvor berücksichtigten Bedrohungen ist, $\mathbb{1} := \sum\limits_{i=1}^{\dim V} e_i \text{ and } a := \sum\limits_{i=1}^{\dim V} a_i e_i \in V$

wobei ai für eine bestimmte Gewichtung des jeweiligen Attributs der Durchführbarkeit der Bedrohung steht.

Betrachtet man t oder c als Vektor von $\mathbb{R}^7$, so hat er die Form

$$t = \begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \\ t_5 \\ t_6 \\ t_7 \end{pmatrix}, c = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{pmatrix}$$

wobei jede Koordinate ti ein Attribut für die Durchführbarkeit der Bedrohung darstellt. Sind eine oder mehrere Koordinaten undefiniert, kann sie auf die Soll-Durchführbarkeit gesetzt werden, die einer vorgegebenen akzeptablen Durchführbarkeit entspricht.

$$M(t, c) = \begin{pmatrix} \min\{t_1, c_1\} \\ \min\{t_2, c_2\} \\ \min\{t_3, c_3\} \\ \min\{t_4, c_4\} \\ \min\{t_5, c_5\} \\ \min\{t_6, c_6\} \\ \min\{t_7, c_7\} \end{pmatrix}$$

$$\mathfrak{F}(M(t,c)) = \frac{< \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix}, \begin{pmatrix} \min\{t_1, c_1\} \\ \min\{t_2, c_2\} \\ \min\{t_3, c_3\} \\ \min\{t_4, c_4\} \\ \min\{t_5, c_5\} \\ \min\{t_6, c_6\} \\ \min\{t_7, c_7\} \end{pmatrix} >}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7}$$

$$= \frac{a_1 \cdot \min\{t_1, c_1\} + a_2 \cdot \min\{t_2, c_2\} + a_3 \cdot \min\{t_3, c_3\} + ... + a_7 \cdot \min\{t_7, c_7\}}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7}$$

Um die Wirkung der gewählten Gegenmaßnahmen zu berücksichtigen, wird die oben definierte Funktion M angewendet. Beispiel: Wenn die Gegenmaßnahmen c und $\tilde{c}$ gegen eine Bedrohung t angewendet werden

$$t = \begin{pmatrix} 1 \\ 5 \\ 2 \\ 5 \\ 3 \\ 3 \\ 4 \end{pmatrix}, c = \begin{pmatrix} 2 \\ 2 \\ 1 \\ 3 \\ x \\ 3 \\ 3 \end{pmatrix}, \tilde{c} = \begin{pmatrix} 3 \\ 3 \\ 3 \\ 1 \\ 3 \\ 2 \\ 1 \end{pmatrix}$$

$$M(t, c, \tilde{c}) = \begin{pmatrix} min\{1,2,3\} \\ min\{5,2,3\} \\ min\{2,1,3\} \\ min\{5,3,1\} \\ min\{3,x,3\} \\ min\{3,3,2\} \\ min\{4,3,1\} \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 1 \\ 1 \\ min\{x,3\} \\ 2 \\ 1 \end{pmatrix}$$

Wobei $x = c_5$ undefiniert ist.

Außerdem wird in diesem Beispiel davon ausgegangen, dass eine durchschnittliche Durchführbarkeit des Ziels von 2 angestrebt wird, wobei x als 2 angenommen wird. x = 2 und n = 2 in $\mathfrak{F}$.

$$\mathfrak{F}(M(t,c,\tilde{c})) = \frac{< \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 1 \\ 1 \\ 2 \\ 2 \\ 1-2\cdot 0.5 \end{pmatrix} >}{1+1+1+1+1+1+1} = \frac{1+2+1+1+2+2+0}{7} = \frac{9}{7} = 1,22$$

Bei der Anwendung von Gegenmaßnahmen werden einige Werte von Aspekten der Durchführbarkeitsattribute für Bedrohungen durch entsprechende Durchführbarkeitsattribute für Gegenmaßnahmen geändert, so dass ein Unterschied zwischen der Gesamtsicherheitsmetrik vor und nach Anwendung einer oder mehrerer Gegenmaßnahmen berechnet werden kann.

Schritt S7

Die Aufgabe besteht darin, einen Satz optimierter Gegenmaßnahmen aus der Liste der identifizierten Gegenmaßnahmen gegen die identifizierten potenziellen Bedrohungen zu bestimmen. Dies kann in **Schritt S7** durch einen Optimierungsprozess erfolgen, der das Ergebnis der Anwendung einer oder mehrerer Gegenmaßnahmen in Bezug auf den Gesamtsicherheitsgewinn berechnet. Die Gegenmaßnahmen können in Bezug auf den Gesamtsicherheitsgewinn in eine Rangfolge von am effektivsten bis am wenigsten effektiv gebracht werden. Als Optimierungsverfahren können herkömmliche Optimierungsalgorithmen verwendet werden, die in der Technik gut bekannt sind.

Bei der Anwendung einer Gegenmaßnahme ist es notwendig, einige Manipulationen am Datensystem vorzunehmen, wie z. B. das Hinzufügen einiger Hardware- oder Softwarekomponenten, die in der Liste der identifizierten Werte des Datensystems berücksichtigt werden müssen. Die hinzugefügten Komponenten wirken sich jeweils auf eine oder mehrere OSI-Schichten aus und führen potenziell zusätzliche Bedrohungen ein, wie sie in der Datenbank abgerufen werden können.

Infolgedessen wird die Durchführung von Gegenmaßnahmen einerseits das Sicherheitsrisiko des Datensystems verringern, andererseits aber zusätzliche Angriffsvektoren als mögliche Bedrohungen hinzufügen. Daher kann eine Verringerung des Niveaus/der Werte der Aspekte der Durchführbarkeitsattribute für Bedrohungen dazu führen, dass zusätzliche Durchführbarkeitsattribute für neue Bedrohungen eingeführt werden.

Im Optimierungsprozess werden die Gegenmaßnahmen in eine Reihenfolge von höchster zu niedrigster Effizienz gebracht. Bei der Bewertung des Gesamtsicherheitsgewinns wird auch die Einführung zusätzlicher potenzieller Bedrohungen durch die betrachteten Gegenmaßnahmen berücksichtigt.

Die nachstehende Tabelle zeigt die Manipulation der Attribute für die Durchführbarkeit von Bedrohungen durch die Anwendung einer Gegenmaßnahme und die sich daraus ergebenden Aspektwerte der Attribute für die Durchführbarkeit von Bedrohungen, wenn die Gegenmaßnahme angewendet wurde.

Bedrohung	Durchführbarkeitsattribut der Bedrohung nach Anwendung einer Gegenmaßnahme

Man in The Middle, um Daten auszulesen	Angriffsvektor: Lokales Netzwerk Komplexität: Sehr einfach -> Sehr komplex (50) Privilegien: Jeder Benutzer-Interaktion: Einfacher Aufwand -> Mehrere Experten (60) Reproduzierbarkeit: Leicht zu reproduzieren (3) -> Muss neu bewertet werden (2) Ausstattung: Standard Eintrittswahrscheinlichkeit: Wahrscheinlich -> Unwahrscheinlich Die Auswirkungen (Schaden) werden reduziert
DDOS-Angriff, Verfügbarkeit	Angriffsvektor: Lokales Netzwerk Komplexität: Sehr einfach (80) -> Mittlere Komplexität Privilegien: Jeder Benutzer-Interaktion: Einfacher Aufwand (90) -> Mittlerer Aufwand Reproduzierbarkeit: Leicht zu reproduzieren Ausstattung: Standard Eintrittswahrscheinlichkeit: Sehr Wahrscheinlich - > Wahrscheinlich Die Auswirkungen werden verringert

Nachdem eine Liste von Gegenmaßnahmen mit hoher bis geringer Effizienz erstellt wurde, können geeignete Gegenmaßnahmen ausgewählt werden, indem die für die Umsetzung der Gegenmaßnahme erforderlichen Ressourcen wie Budget, Arbeitskräfte, Fähigkeiten, Zeit, Verarbeitungskapazität, Speicherkapazität und ähnliches berücksichtigt werden. Wenn die Ressourcen begrenzt sind, wird die Effizienz der Gegenmaßnahme in Kombination mit einer Kostenfunktion betrachtet, mit dem Ziel, die Effizienz angesichts der begrenzten Ressourcen zu maximieren. Das Ergebnis kann die Reihenfolge der durchzuführenden Gegenmaßnahmen oder, bei begrenzten Ressourcen, die geeignete Gegenmaßnahme sein, um die höchste Effizienz im Hinblick auf den Sicherheitsgewinn zu erreichen.

Claims/Anforderungen

1. Computerimplementiertes Verfahren zum Auswählen von Gegenmaßnahmen für potentielle Bedrohungen von Werten eines Datensystems (2), das die folgenden Schritte umfasst:
   a. Bereitstellen (S1) einer Konfiguration des Datensystems einschließlich seiner Anlagen, einschließlich Geräten (21, 22, 23, 24, 25, 26, 27, 28, 29), Software, Daten, Datenübertragungen und deren Verbindungen;
   b. Abrufen (S2) eines Satzes relevanter OSI-Schichten, auf denen bekannte Sicherheitsvektoren existieren können, für jeden Asset aus einer Datenbank (14),
   c. für jede abgerufene OSI-Schicht jedes Objekts, Abrufen (S3) von potenziellen Bedrohungen aus der Datenbank (14), die jeweils einem oder mehreren Sicherheitsattributen zugeordnet sind, die jeweils ein Ziel der Cybersicherheit definieren, wobei die potenziellen Bedrohungen einem oder mehreren Bedrohungsdurchführbarkeitsattributen zugeordnet sind, die jeweils einen Grad eines Durchführbarkeitsaspekts angeben, der ein durch die jeweilige potenzielle Bedrohung auferlegtes Sicherheitsrisiko ausgleicht;
   d. Verwenden der Datenbank, Zuordnen (S4) von mindestens einer Gegenmaßnahme aus einem Satz von Gegenmaßnahmen zu jeder der potenziellen Bedrohungen, wobei jede Gegenmaßnahme mindestens ein Gegenmaßnahme-Durchführbarkeitsattribut hat, das jeweils ein Niveau eines Durchführbarkeitsaspekts angibt, das erreicht wird, wenn die Gegenmaßnahme auf die potenzielle Bedrohung angewendet wird, wobei die Gegenmaßnahme geeignet ist, das Sicherheitsrisiko der jeweiligen potenziellen Bedrohung in einem oder mehreren Aspekten von Bedrohungs-Durchführbarkeitsattributen zu reduzieren;
   e. Automatisches Durchführen (S5) einer Optimierung, um eine oder mehrere Gegenmaßnahmen aus dem Satz von Gegenmaßnahmen auszuwählen, so dass die ausgewählten Gegenmaßnahmen ausreichen, um ein Gesamtsicherheitsrisiko unter ein gegebenes Niveau des Sicherheitsrisikos zu reduzieren.
2. Verfahren nach Anforderung 1, wobei die Sicherheitsattribute mindestens eines der folgenden umfassen: Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit.
3. Verfahren nach Anforderung 1 oder 2, wobei die Aspekte der Durchführbarkeit mindestens einen der folgenden Aspekte umfassen: Angriffsvektor, Komplexität, Privilegien, Benutzerinteraktion, Reproduzierbarkeit, Ausrüstung und Wahrscheinlichkeit.
4. Verfahren nach einem der Anforderungen 1 bis 3, wobei das Gesamtsicherheitsrisiko mittels einer Gesamtsicherheitsmetrik bewertet wird, die auf der Grundlage der Durchführbarkeitsattribute der Bedrohungen aller potenziellen Bedrohungen und des Durchführbarkeitsattributs der Gegenmaßnahmen aller in Betracht gezogenen Gegenmaßnahmen berechnet wird, wobei die Optimierung auf der Grundlage einer Minimierung einer Kostenfunktion durchgeführt wird, die von der Gesamtsicherheitsmetrik abhängt.
5. Verfahren nach Anforderung 4, wobei die Gesamtsicherheitsmetrik durch Gewichtung der Durchführbarkeitsstufen berechnet wird.
6. Verfahren nach Anforderung 4 oder 5, wobei die Kostenfunktion der Optimierung von den Ressourcen abhängt, die für die Implementierung der jeweils betrachteten einen oder mehreren Gegenmaßnahmen benötigt werden, insbesondere von Zeit, Material, Budget, Arbeitskräften, Fähigkeiten, Verarbeitungskapazität und Speicherkapazität.
7. Verfahren nach einem der Anforderungen 1 bis 6, wobei die ausgewählten Gegenmaßnahmen signalisiert oder durchgeführt werden.

8. Verfahren nach einem der Anforderungen 1 bis 7, wobei die ausgewählten Gegenmaßnahmen sukzessive durch iterative Durchführung von Optimierungsschritten jeweils nach Annahme der Anwendung der zuvor ausgewählten Gegenmaßnahmen bestimmt werden.
9. Verfahren nach Anforderung 8, wobei das Annehmen der Anwendung der zuvor ausgewählten Gegenmaßnahmen das Hinzufügen von einem oder mehreren weiteren Assets umfasst, die durch die angenommene Anwendung der Gegenmaßnahme verursacht werden, wobei mindestens eine neue Bedrohung und mindestens eine neue Gegenmaßnahme mit dem einen oder den mehreren weiteren Assets verbunden ist, wobei die nächste Iteration der Optimierung die mindestens eine neue Bedrohung und mindestens eine neue Gegenmaßnahme berücksichtigt.
10. Verfahren nach einem der Anforderungen 1 bis 9, wobei die Gegenmaßnahmen eines oder mehrere der folgenden Elemente umfassen: SecOC - Secure on board communication, Installation oder Verbesserung einer Firewall, Installation oder Verbesserung eines Intrusion Detection Systems, Installation oder Verbesserung eines Hardware-Sicherheitsmoduls, Einrichtung einer synchronen Verschlüsselung oder einer asynchronen Verschlüsselung, Anwendung von Prüfsummen oder Rolling Codes, Bereitstellung einer Abschirmung und/oder Versiegelung, Verwendung einer 2-Faktor-Authentifizierung oder -Autorisierung für die Hardware (Bindung der Hardware), Installation oder Verbesserung eines kritischen Luftspaltsystems, Anwendung einer Zero-Trust-Netzwerkarchitektur, Verwendung sicherer Bootloader, Installation oder Verbesserung manipulationssicherer Hardware, Anwendung einer Netzwerksegmentierung, Anwendung eines sicheren Bootvorgangs und Anwendung einer Zugriffskontrolle.
11. Eine Vorrichtung, die so konfiguriert ist, dass sie das Verfahren nach einem der Anforderungen 1 bis 10 durchführt.
12. Ein Computerprogramm, das so eingerichtet ist, dass es das Verfahren nach einem der Anforderungen 1 bis 10 ausführt.
13. Ein maschinenlesbares Speichermedium, das das Computerprogramm nach Anforderung 12 speichert.

Zusammenfassung

Die vorliegende Erfindung bezieht sich auf ein computerimplementiertes Verfahren zur Auswahl von Gegenmaßnahmen für potentielle Bedrohungen von Anlagen eines Datensystems, das die folgenden Schritte umfasst:

- Bereitstellen einer Konfiguration des Datensystems einschließlich seiner Anlagen und ihrer Verbindungen;
- Abrufen eines Satzes relevanter OSI-Schichten, auf denen bekannte Sicherheitsvektoren existieren können, für jede Anlage aus einer Datenbank,
- Abrufen von potentiellen Bedrohungen aus der Datenbank für jede abgerufene OSI-Schicht jeder Anlage, die jeweils einem oder mehreren Sicherheitsattributen zugeordnet sind, die jeweils ein Ziel der Cybersicherheit definieren, wobei die potentiellen Bedrohungen einem oder mehreren Bedrohungsdurchführbarkeitsattributen zugeordnet sind, die jeweils einen Grad eines Durchführbarkeitsaspekts angeben, der ein durch die jeweilige potentielle Bedrohung auferlegtes Sicherheitsrisiko ausgleicht;
- Verwenden der Datenbank, Zuordnen von mindestens einer Gegenmaßnahme aus einem Satz von Gegenmaßnahmen zu jeder der potenziellen Bedrohungen, wobei jede Gegenmaßnahme mindestens ein Gegenmaßnahme-Durchführbarkeitsattribut hat, das jeweils ein Niveau eines Durchführbarkeitsaspekts angibt, das erreicht wird, wenn die Gegenmaßnahme auf die potenzielle Bedrohung angewendet wird, wobei die Gegenmaßnahme geeignet ist, das Sicherheitsrisiko der jeweiligen potenziellen Bedrohung in einem oder mehreren Aspekten von Bedrohungs-Durchführbarkeitsattributen zu reduzieren;
- Automatisches Durchführen einer Optimierung, um eine oder mehrere Gegenmaßnahmen aus dem Satz von Gegenmaßnahmen auszuwählen, so dass die ausgewählten Gegenmaßnahmen ausreichen, um ein Gesamtsicherheitsrisiko unter ein gegebenes Niveau des Sicherheitsrisikos zu reduzieren.

Berichtsblatt

1. ISBN oder ISSN	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht
3. Titel **Verfahren und Plattform zur Bestimmung von Gegenmaßnahmen gegen Sicherheitsprobleme und zum Schutz der Industrieobjekte**	
4. Autor(en) [Name(n), Vorname(n)] Oscar Angress Jürgen Vollmer	5. Abschlussdatum des Vorhabens 30.6.2024
	6. Veröffentlichungsdatum 23.7.2024
	7. Form der Publikation Patentanmeldung
8. Durchführende Institution(en) (Name, Adresse) Primary Target GmbH Freimanner Strasse 14 85737 Ismaning SQ Software GmbH Virchow Str. 7 Würzburg, 97072	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 16KIS1664
	11. Seitenzahl
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben
	14. Tabellen
	15. Abbildungen
16. Zusätzliche Angaben Die F&E Tätigkeiten wurden von zwei Firmen und ihren international tätigen Mitarbeitern durchgeführt.	
17. Vorgelegt bei (Titel, Ort, Datum)	

18. Kurzfassung

Industrielle Produkte sind heute zunehmend komplex und bestehen aus einfachen Bauteilen, Baugruppen, elektronischen Komponenten und Netzwerken. Diese Komponenten können Hardware und/oder Software für mindestens eine der Funktionen Datenverarbeitung, Datenübertragung, Datenmanagement usw. enthalten. Diese Komponenten von Datensystemen sind in der Regel Bedrohungen ausgesetzt und weisen bekannte Schwachstellen im Bereich der Cyber-Sicherheit auf.
Die Risikobewertung wird werden Sicherheitsgegenmaßnahmen, die es Benutzern von Sicherheits- und Compliance-Systemen ermöglicht, Risiken und Schwachstellen in ihrer Umgebung mit dem zusätzlichen Kontext zu betrachten, welche anderen abschwächenden Sicherheitsgegenmaßnahmen mit dieser Schwachstelle verbunden und innerhalb der gesamten Sicherheitsarchitektur anwendbar und/oder verfügbar sind. Darüber hinaus ermöglicht die Plattform den Nutzern, eine oder mehrere Maßnahmen zu ergreifen, die von der Steuerung des Betriebs einer Sicherheitsgegenmaßnahme zu Abschwächungszwecken bis hin zur einfachen Dokumentation des Bekanntheitsgrads einer bestehenden Sicherheitsgegenmaßnahme reichen.
Darüber hinaus offenbart das Dokument US 2014/0137257 A1 ein Verfahren zur Bewertung eines Risikos von einem oder mehreren Assets innerhalb einer betrieblichen Technologieinfrastruktur, das die folgenden Schritte umfasst: Bereitstellen einer Datenbank, die Daten enthält, die sich auf den einen oder die mehreren Assets beziehen, Berechnen einer Bedrohungsbewertung für den einen oder die mehreren Assets unter Verwendung eines oder mehrerer Prozessoren, die kommunikativ mit der Datenbank verbunden sind, Berechnen einer Schwachstellenbewertung für den einen oder die mehreren Asset unter Verwendung des einen oder der mehreren Prozessoren, Berechnen einer Auswirkungsbewertung für den einen oder die mehreren Asset unter Verwendung des einen oder der mehreren Prozessoren; und Bestimmen des Risikos der einen oder mehreren Anlagen auf der Grundlage der Bedrohungsbewertung, der Schwachstellenbewertung und der Auswirkungsbewertung unter Verwendung des einen oder der mehreren Prozessoren.

19. Schlagwörter	
20. Verlag	21. Preis