Artikelserie: Modellierung von Cyberbedrohungen (Threat Modeling) im industriellen Umfeld

@-Yet Industrial IT Security
52078 Aachen
Neuenhofstrasse 194

www.add-yet-iis.de

Inhaltsverzeichnis

Threat Modeling - Beitrag 1

Einleitung

Die Erfahrung aus den letzten Wochen und Monaten zeigt, dass auch industrielle Anlagen verstärkt im Fokus von Cyberkriminellen stehen. Dabei ist der Sektor, in dem die Anlage arbeitet und die Größe des angegriffenen Unternehmens nicht mehr ausschlaggebend, ob eine Angriff stattfindet oder nicht.

Die Gesetzgebung zieht nach. Verordnungen und Richtlinien der EU (z.B. NIS2, CRA, Maschinen-verordnung) sollen hier für mehr Cybersicherheit sorgen. Dabei helfen Standards und Best Practices (z.B. IEC 62443, ISO 27001, BSI Grundschutz, NIST) die notwendigen Maßnahmen zu identifizieren.

Aber genau hier liegt das Problem: Wogegen will ich mich schützen? Was sind mögliche Angriffe gegen die zu schützende Anlage?

Cybersicherheit kostete Geld. Sowohl Technik als auch Personal müssen hier im Zusammenspiel eingesetzt werden, um das Ziel *Security* zu erreichen. Daher wäre es interessant zu wissen, was für Angriffe sind denn überhaupt möglich und wahrscheinlich? Ist das bekannt, können die Mittel punktgenau eingesetzt werden. Hierzu kann sehr gut Threat Modeling (*Bedrohungsmodellierung*) eingesetzt werden.

In den folgenden Beiträgen wird gezeigt, was eine Bedrohungsmodellierung ist, wie sie im OT Umfeld eingesetzt werden kann und wie @-yet IIS Sie bei der Durchführung unterstützt.

Threat Modeling - Beitrag 2

Bei der Bedrohungsmodellierung handelt es sich um eine Reihe von Aktivitäten zur Verbesserung der Sicherheit durch die Identifizierung von Bedrohungen und die anschließende Festlegung von Gegenmaßnahmen zur Verhinderung oder Abschwächung der Auswirkungen von Bedrohungen auf das System. Es ist ein analytischer Prozess. Eine Bedrohung ist ein potenzielles oder tatsächliches unerwünschtes Ereignis, das böswillig (wie z.B. ein DoS-Angriff) oder zufällig (z.B. Ausfall eines Speichergeräts) sein kann. Die Bedrohungsmodellierung ist eine geplante Aktivität zur Identifizierung und Bewertung von Anwendungsbedrohungen und Schwachstellen. Dieses Verfahren kann sowohl in den frühen Phasen des Lebenszyklus eingesetzt werden (*Secure-by-Design*), aber auch bei schon bestehenden, laufenden Systemen (Brown field) verwendet werden.

Typischerweise wurde eine Bedrohungsmodellierung bisher hauptsächlich bei Software eingesetzt und findet erst langsam den Weg in die OT. Aber auch hier kann sie mit großem Nutzen eingesetzt werden. Dabei ist neben der „*Security*“ auch die „*Safety*“ mit zu berücksichtigen!

Wie die Bedrohungsmodellierung sinnvoll in der OT eingesetzt werden kann um mögliche und realistische Angriffe zu erkennen, soll in dieser Artikelserie beschrieben werden.

Es wird auszugsweise gezeigt, wie die Bedrohungsmodellierung bei der Verwendung des Standards **IEC 62443** eingebunden werden kann. Aber auch bei anderen Vorgehensweisen (Grundschutz, Cyber Security Framework) liefert die Bedrohungsmodellierung wichtige Informationen zur Bestimmung von sinnvollen Cyber-Sicherheitsmaßnahmen.

Threat Modeling - Beitrag 3

Die Beteiligten

Es ist wichtig, darauf hinzuweisen, dass die Modellierung von Bedrohungen keine **rein** analytische Aufgabe ist. Es handelt sich um einen Prozess, der die Kommunikation und das gemeinsame Verständnis zwischen den verschiedenen Beteiligten erleichtert. Im Vergleich zu softwarebasierten Systemen verfügen Automatisierungssysteme über vielfältigere Hardware-, Software- und Kommunikationskomponenten, die eine physische Aufgabe erfüllen, und erfordern daher die Einbeziehung unterschiedlicher Interessengruppen, wie z. B. *Betreiber*, die sich mit den physischen Prozessen befassen, oder *heterogenere Entwicklungsteams* mit unterschiedlichem Hintergrund neben den *IT*- oder *OT-Systembetreibern*.

Daher müssen die Methoden der Bedrohungsmodellierung, die hauptsächlich für Software entwickelt wurden, an die Stakeholder-Struktur von Automatisierungsumgebungen angepasst werden.

Weiterhin ist es für die Bedrohungsmodellierung sinnvoll, erfahrene Pentester und IT Forensiker mit im Team zu haben. Sie kennen viele Angriffsarten, vor allem aber kennen Sie reale Angriffswege. Nicht jede Schwachstelle führt direkt zu einer Gefährdung. Dazu muss es auch eine Bedrohung geben. Wer reale Angriffe kennt, ist auch in der Lage, reale Bedrohungen einzuschätzen. Wenn das der Fall ist, kann sich die Bedrohungsanalyse auf die Angriffe konzentrieren, die wirklich relevant für eine Anlage sind. Das hilft u.a., die Anzahl der zu betrachtenden Bedrohungen in einem überschaubaren Maß einzuschränken. Ansonsten kann es passieren, dass zu viele Bedrohungen das Ergebnis unübersichtlich machen.

Ein wichtiger Standard bezüglich OT Security ist der IEC 62443. Wie dieser Standard bei einer Bedrohungsmodellierung eingesetzt werden kann, erfahren Sie im nächsten Beitrag dieser Serie.

Threat Modeling - Beitrag 4

IEC 62443

Grundlagen

Der Standard IEC 62443 legt den Grundstein für eine ganzheitliche Betrachtung von Industrial Security im gesamten Lebenszyklus von Automatisierungslösungen. Er wendet sich an Betreiber, Integratoren und Hersteller und liefert einen globalen Überblick über aller relevanten Aspekte der OT Security.

Im Rahmen dieser Artikelserie soll eine Bedrohungsanalyse, basierend auf dem Standard IEC 62443, beschrieben werden.

Im Standard werden Sicherheitslevel (*SL*) beschrieben und ein Anlagenbetreiber kann mit der Auswahl eines Sicherheitslevels festlegen, gegen welche Art von Cyber-Angreifern er sich schützen will. Es gibt 4 Sicherheitslevel (1-4).

***Tabelle** – Sicherheitslevel in IEC 62443*

Sicherheitslevel	Schutz gegen…
1	Zufällige Fehlanwendung
2	Absichtliche Versuche mit einfachen Mitteln
3	Wie SL2, jedoch mit erweiterten Kenntnissen und erweiterten Mitteln
4	Wie SL3, jedoch mit spezifischen Kenntnissen und erheblichen Mittel

SL 2 schützt gegen sogenannte *Script Kiddies*, **SL 3** gegen *professionelle kriminelle Hackergruppen* und **SL 4** gegen *staatliche Angreifer*. Der Mehraufwand an Technik und Organisation zwischen den Sicherheitsleveln ist **nicht unerheblich**. Damit verbunden sind auch die zugehörigen Kosten.

Welche konkreten Anforderungen der Standard zur Behandlung von Bedrohungen stellt, erfahren Sie im nächsten Beitrag dieser Serie.

Threat Modeling - Beitrag 5

In den Teilen **IEC 62443-3-2 Abschnitt ZCR5.1** (***Z**one and **C**onduit **R**equirements*) wird explizit gefordert Bedrohungen zu identifizieren. Die Informationen fließen in eine detaillierte Risikobeurteilung mit ein.

Im Teil **IEC 62443-4-1**[1] wird ebenfalls als grundlegender Aspekt die Durchführung einer Risikobeurteilung gefordert. Im Abschnitt **SR-2** (***S**ystem **R**equirement*) wird explizit ein Prozess gefordert, der sicherstellt, *dass alle Produkte ein für den aktuellen Entwicklungsumfang des Produkts spezifisches Bedrohungsmodell mit den folgenden Merkmalen (sofern anwendbar) aufweisen müssen:*

a)	einen ordnungsgemäßen Fluss der kategorisierten Informationen im gesamten System
b)	Vertrauensgrenzen
c)	Prozesse
d)	Datenspeicher
e)	Wechselwirkungen mit externen Instanzen
f)	interne und externe Kommunikationsprotokolle, die im Produkt implementiert sind
g)	von außen zugängliche physische Anschlüsse einschließlich Debug-Anschlüsse
h)	Leiterplattenanschlüsse wie JTAG-Anschlüsse oder Debug-Anschlussleisten, die zum Angriff auf die Hardware genutzt werden können
i)	mögliche Angriffsvektoren einschließlich von Angriffen auf die Hardware, soweit anwendbar
j)	mögliche Bedrohungen und deren Schweregrad nach einer Festlegung durch ein Verwundbarkeitsbewertungssystem (z. B. CVSS)*
k)	Abschwächungsmaßnahmen und/oder Behandlung jeder Bedrohung
l)	ermittelte sicherheitsbezogene Probleme
m)	äußere Abhängigkeiten in Form von Treibern oder Fremdanwendungen (nicht vom Hersteller entwickelter Code), die mit der Anwendung verknüpft werden.

CVSS * [2]

***Tabelle** - Merkmale für ein spezifisches Bedrohungsmodell*

Wie diese Anforderungen erfüllt werden können, erfahren Sie im nächsten Beitrag dieser Serie.

[1] DIN EN IEC 62443-4-1 (VDE 0802-4-1): 2018-10

[2] CVSS – Common Vulnerability Scoring System; www.first.org/cvss

Threat Modeling - Beitrag 6

Für die Erfüllung der Anforderungen sind besonders die Teile **IEC 62443-3-3** und **IEC 62443-4-2** interessant.

IEC 62443-3-3 beschreibt allgemeine Systemsicherheitsanforderungen wie Authentifizierung, Datenvertraulichkeit und Systemintegrität.

Dabei werden Anforderungen zur IT-Sicherheit von industriellen Automatisierungslösungen gemäß sieben grundlegender Anforderungen (*Foundational Requirements FR 1-7*) festgelegt.

Das sind:

- **FR 1** – Identifizierung und Authentifizierung
- **FR 2** – Nutzungskontrolle
- **FR 3** – Systemintegrität
- **FR 4** – Vertraulichkeit der Daten
- **FR 5** – Eingeschränkter Datenfluss
- **FR 6** – Rechtzeitige Reaktion auf Ereignisse
- **FR 7** – Ressourcenverfügbarkeit

Zu einer *grundlegenden* Systemanforderung werden teilweise weitere weitergehende Anforderungen aufgeführt (*Requirement enhancements, RE*), die abhängig vom gewählten Sicherheitslevel sind.

Weiterhin werden in dieser Norm Randbedingungen genannt, die typisch für industrielle Automatisierungssysteme sind, beispielsweise der Erhalt von Realzeiteigenschaften bei Erkennung eines Cyber-Sicherheitsvorfalls, die Aufrechterhaltung von Sicherheitsfunktionen oder der Weiter-betrieb bei Denial-of-Service-Angriffen.

IEC 62443-4-2[3] spezifiziert die technischen Komponentenanforderungen (*component requirements, CR*) für die Absicherung der einzelnen Komponenten eines ICS-Netzes. Diese Anforderungen werden aus den Systemanforderungen nach **IEC 62443-3-3** hergeleitet.

IEC 62443-1-1 beschreibt Konzepte und Modelle, die im Weitern zum Einsatz kommen. Welche das sind, erfahren Sie im nächsten Beitrag dieser Serie.

[3] DIN EN IEC 62443-4-2 (VDE 0802-4-2):2019-12

Threat Modeling - Beitrag 7

Der Standard **IEC 62443-1-1**[4] beschreibt einige Konzepte und Modelle, die in den weitere Teilen des Standards verwendet werden. Dazu gehören z.B. *Least Privilege*, *Defense in Depth*, *Threat-Risk-Assessment* und *Zones and Conduits*.

Least Privilege bedeutet, dass einem Benutzer oder einer Anwendung nur die Privilegien eingeräumt werden, die zur Erfüllung der notwendigen Aufgaben erforderlich sind.

In der Regel ist es nicht möglich, die Sicherheitsziele durch den Einsatz einer einzigen Gegenmaßnahme oder Technik zu erreichen. Ein besserer Ansatz ist die Anwendung des Konzepts *Defense in Depth*, bei dem mehrere Schutzmaßnahmen schicht- oder stufenweise eingesetzt werden.

Im Rahmen des Prozesses des *Threat-Risk-Assessments* (Bedrohungs-Risiko-Bewertung) sind die Vermögenswerte Risiken ausgesetzt. Diese Risiken werden wiederum durch den Einsatz von Gegenmaßnahmen minimiert, die zur Behebung von Schwachstellen eingesetzt werden, die von verschiedenen Bedrohungen genutzt oder ausgenutzt werden.

Jede Situation hat ein anderes akzeptables Sicherheitsniveau. Bei großen oder komplexen Systemen ist es unter Umständen nicht praktikabel oder notwendig, für alle Komponenten das gleiche Sicherheitsniveau anzuwenden. Die Unterschiede können durch das Konzept einer *Zone* ausgeglichen werden, die als logische oder physische Gruppierung von physischen, informationstechnischen und anwendungsbezogenen Ressourcen mit gemeinsamen Sicherheitsanforderungen definiert ist.

Informationen müssen in eine Sicherheitszone hinein, aus dieser heraus und innerhalb dieser Zone fließen. Um die Sicherheitsaspekte der Kommunikation abzudecken definiert diese Norm eine besondere Art von Sicherheitszone: ein Kommunikations-*Conduit*. Conduits können Einheiten innerhalb einer Zone, oder verschiedene Zonen miteinander verbinden und kontrollieren dabei die Kommunikation.

Wie der Standard IEC 62443 unter Einbeziehung einer Bedrohungsmodellierung verwendet werden kann, erfahren Sie erfahren im nächsten Beitrag dieser Serie.

[4] IEC TS 62443-1-1:2009-07

Threat Modeling - Beitrag 7

Ablauf von IEC 62443 und Einbeziehung einer Bedrohungsmodellierung

Bei der Entwicklung einer neuen Anlage sieht der Ablauf in der IEC 62443 folgendermaßen aus:

1. Bewertungsphase
2. Entwurf-, Technik- und Umsetzungsphase
3. Betriebs- und Instandhaltungsphase

In der den folgenden Abbildungen sind die *Bewertungsphase*, die *Entwurfs-, Technik und Umsetzungsphase* und die Betriebs- und Instandhaltungsphase im Detail dargestellt.

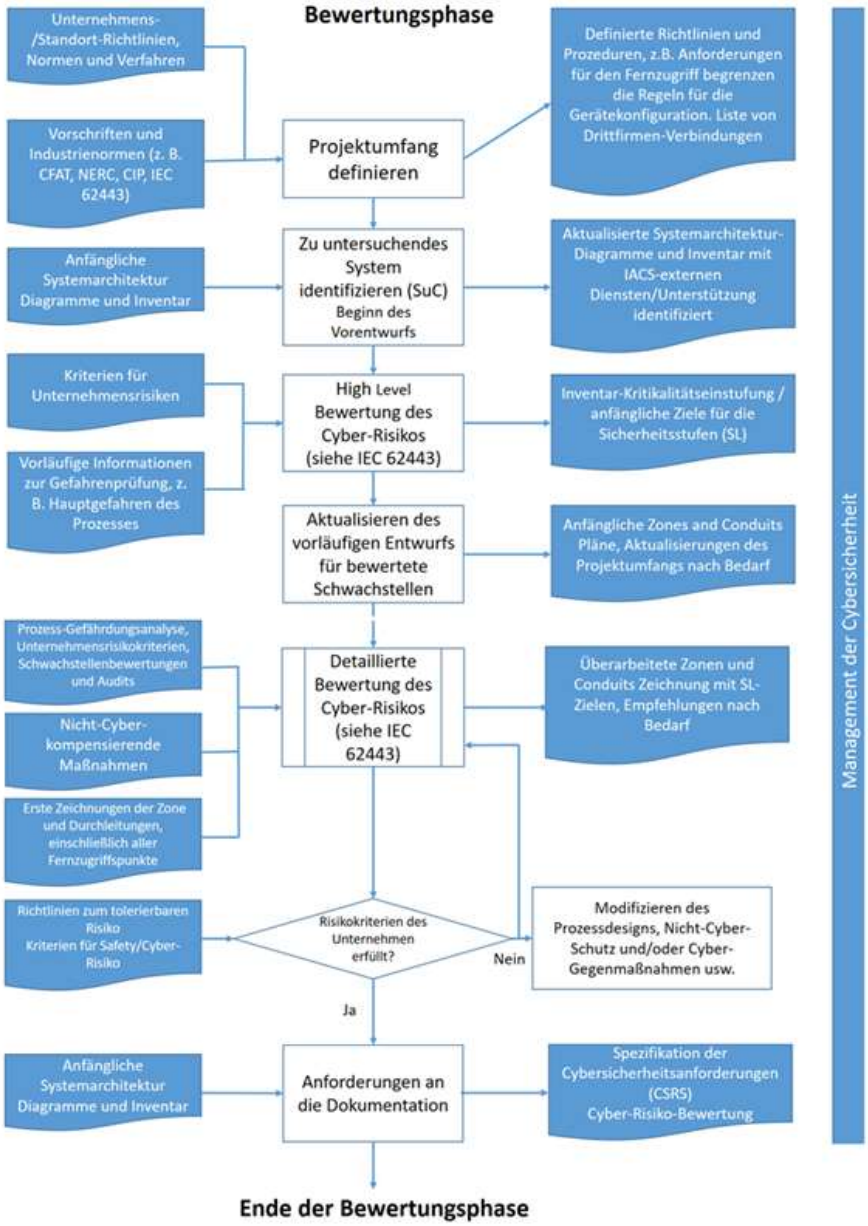

Abbildung 1: *Bewertungsphase*

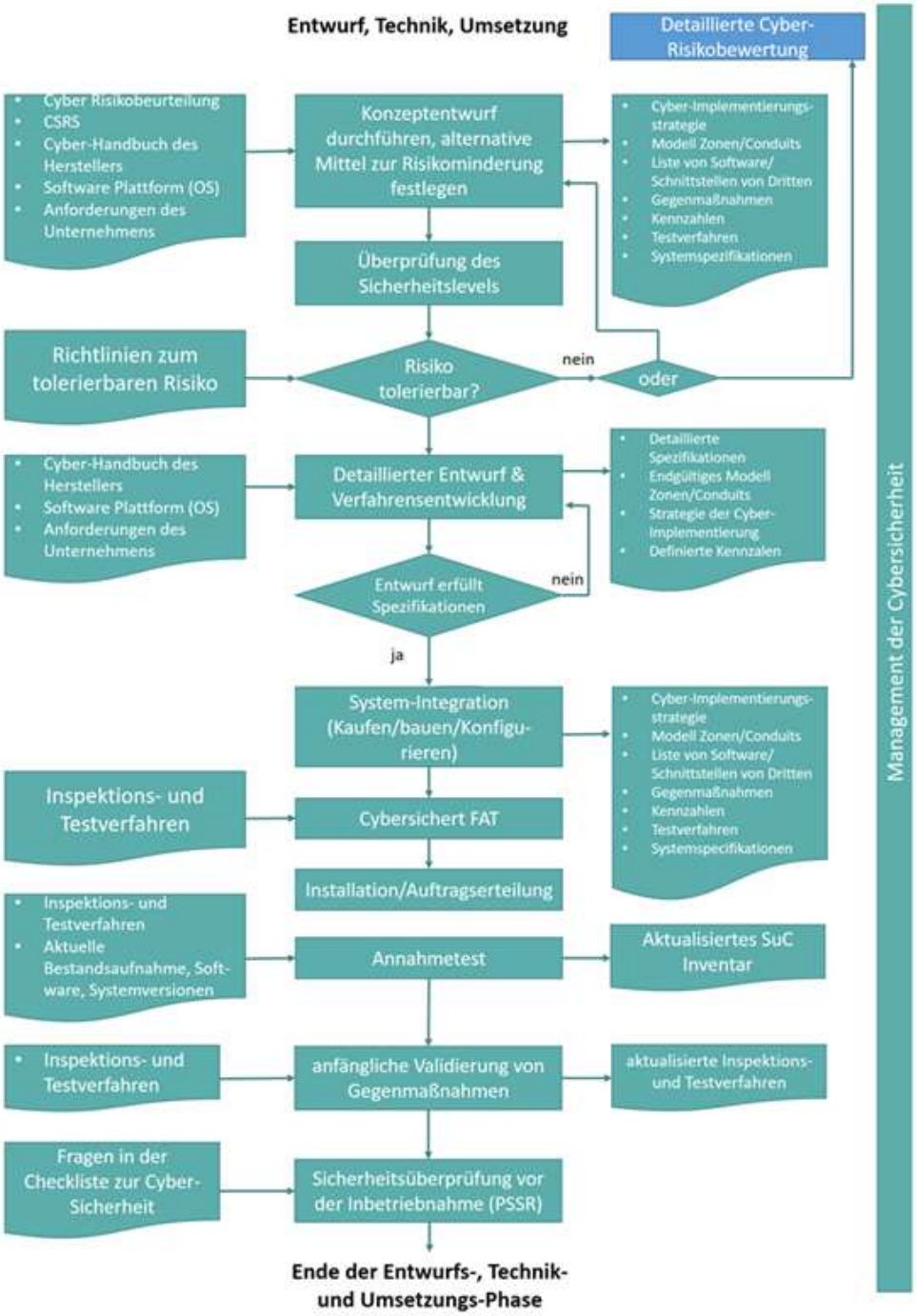

Abbildung 2: *Entwurfs-, Technik- und Umsetzungsphase*

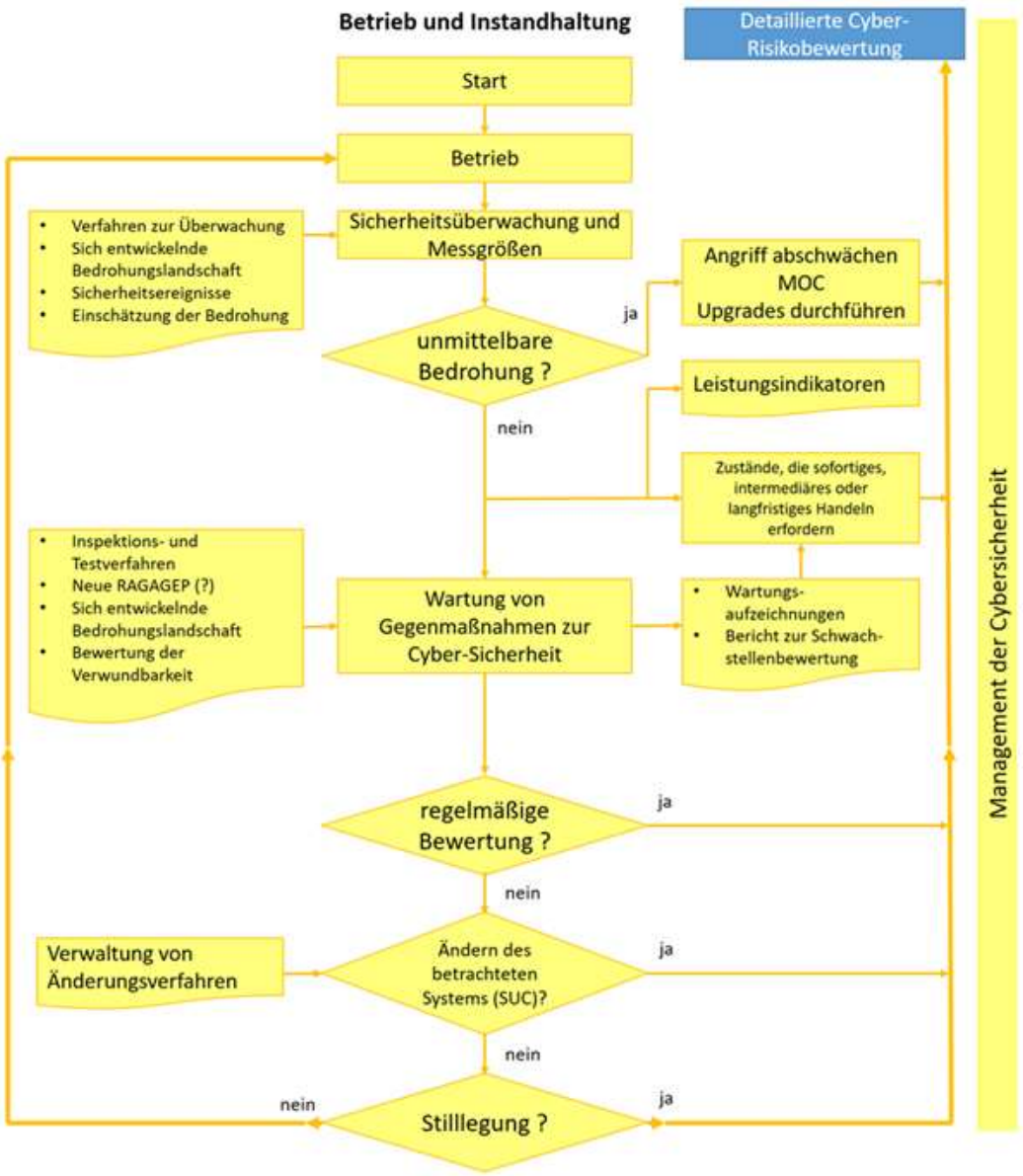

Abbildung 3: *Betriebs- und Instandhaltungsphase*

Die Phasen können auch (teilweise) in eine existierende Produktion eingeführt werden. Natürlich sind einige Teile bei einer bereits laufenden Anlage nicht mehr änderbar.

Wie mit dieser Situation zu verfahren ist, erfahren Sie im nächsten Beitrag dieser Serie.

Threat Modeling - Beitrag 8

Wenn es Teile in einer existierenden Anlage gibt, die nicht dem Standard entsprechen, aber auch nicht geändert werden können (End-of-life erreicht, Hersteller existiert nicht mehr, es gibt keine Patches, usw), dann müssen kreative Lösungen gefunden werden.

Der Standard beschreibt sogenannte *Kompensierende Maßnahmen*. Ist es nicht möglich eine Schwachstelle zu eliminieren (z.B. eine SPS, die unbedingt erforderlich ist, hat eine Schwachstelle und es gibt keinen Patch vom Hersteller), kann sie eventuell isoliert werden. Eine Schwachstelle, die für einen Angreifer nicht erreichbar ist (es gibt keine Bedrohung), stellt keine Gefährdung da!

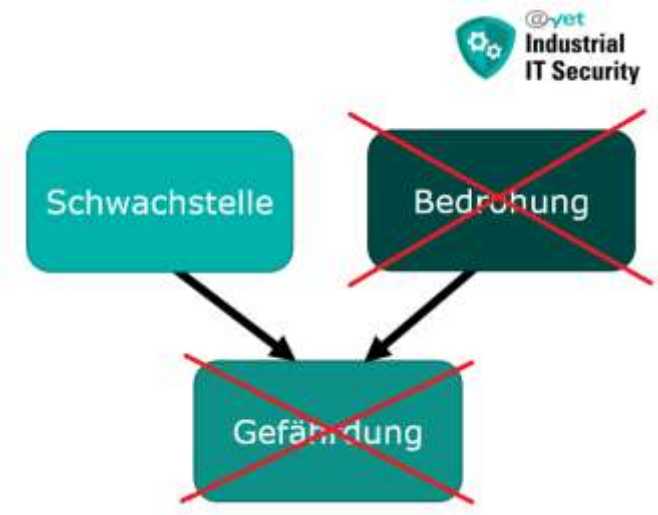

Abbildung 1: *Schwachstelle + Bedrohung = Gefährdung*

Wie IEC 62443 in den Lifecycle einer existierende Produktion eingeführt werden kann, erfahren Sie im nächsten Beitrag dieser Serie.

Threat Modeling - Beitrag 9

Im folgenden Bild sehen Sie, wie IEC 62443 in den Lifecycle einer existierenden Produktion eingeführt werden kann. Die Produktion befindet sich in der Betriebsphase. Nun soll Security nach IEC 62443 eingeführt werden.

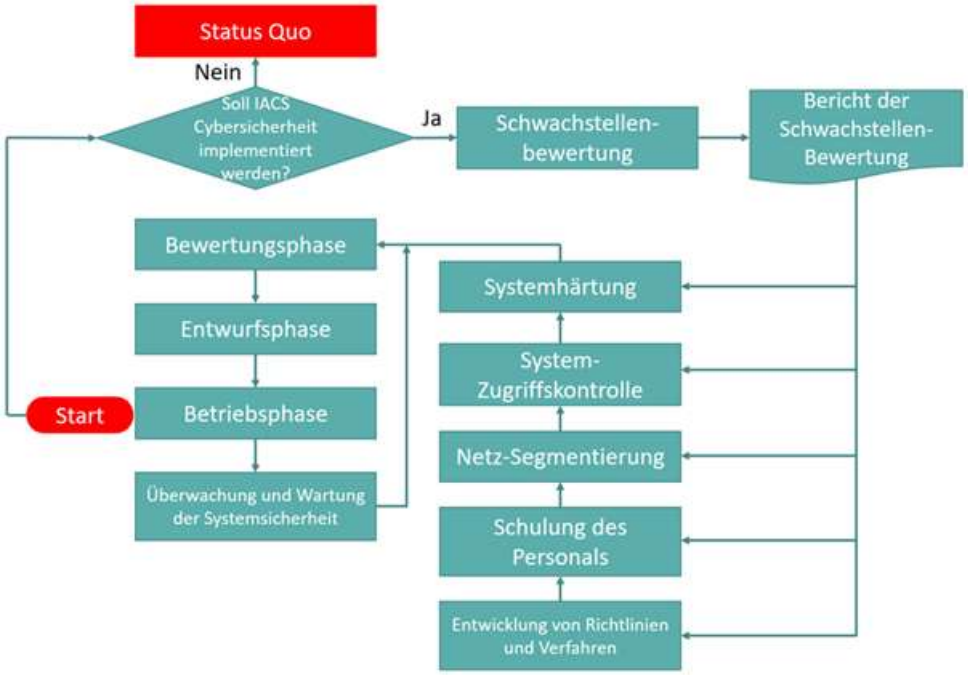

Abbildung 1: *Lifecycle einer Produktionsanlage*

Wie die Anlagenarchitektur aussehen sollte, erfahren Sie im nächsten Bericht dieser Serie.

Threat Modeling - Beitrag 10

Der Aufbau und die Architektur der Automatisierungsanlage hat einen sehr großen Einfluss auf die Sicherheit. Daher liefert der Standard **IEC 62443-3-2** Anforderungen für die Einführung und den Betrieb von *Zonen und Conduits* (Zones and Conduit Requirements, ZCR).

Im folgenden Bild ist der Ablauf für den Einsatz der Anforderungen in der Konzeptphase aufgezeigt:

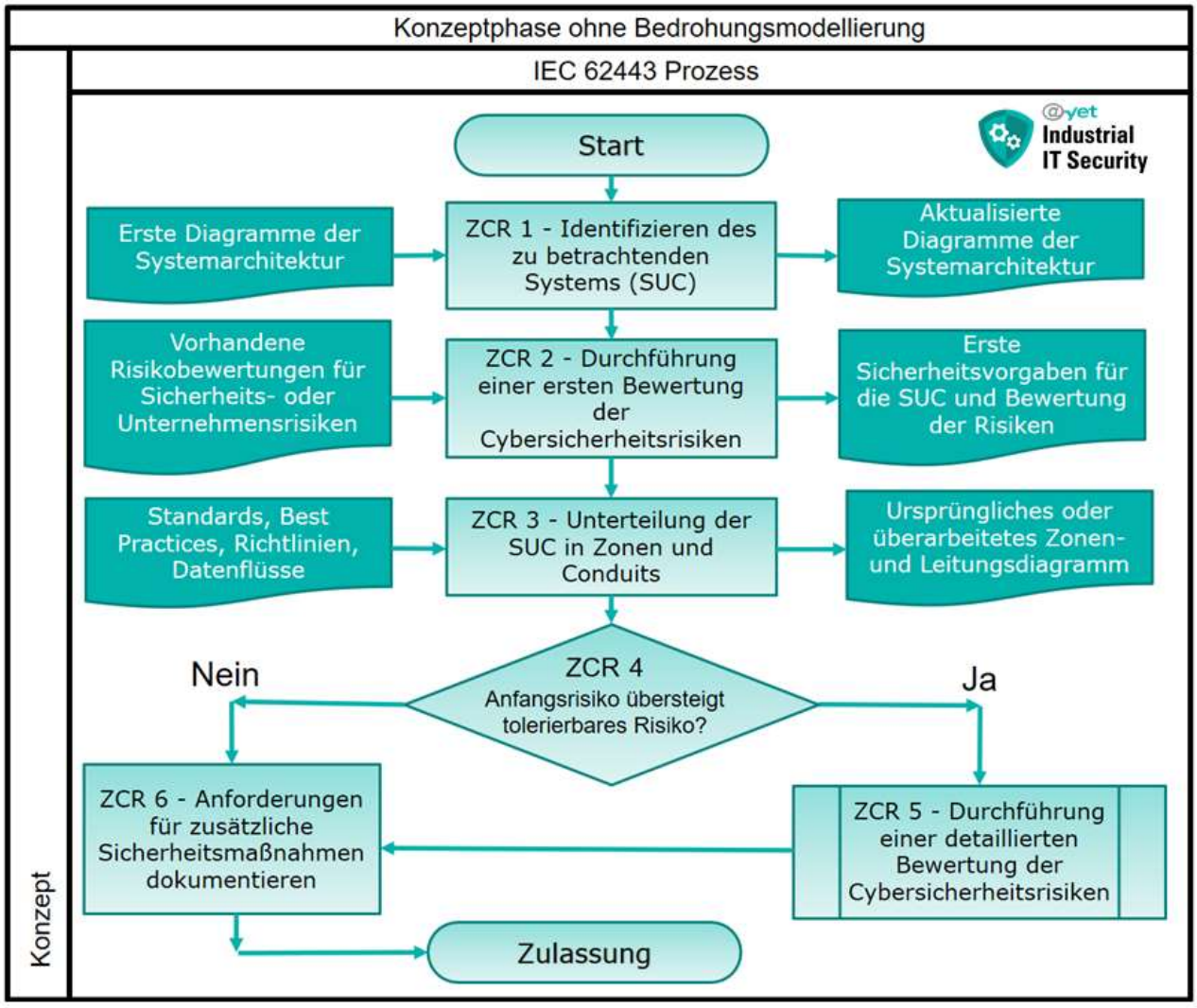

Abbildung 1: *Konzeptphase ohne Bedrohungsmodellierung*

Wie sie eine Bedrohungsmodellierung in diesen Ablauf integrieren können, erfahren Sie im nächsten Beitrag dieser Serie.

Threat Modeling - Beitrag 11

In dem im letzten Beitrag gezeigten Ablauf, wo auch Risiken behandelt werden, lässt sich eine Bedrohungsmodellierung sehr gut einbauen. Wie das genau aussieht, wird im folgenden Bild gezeigt:

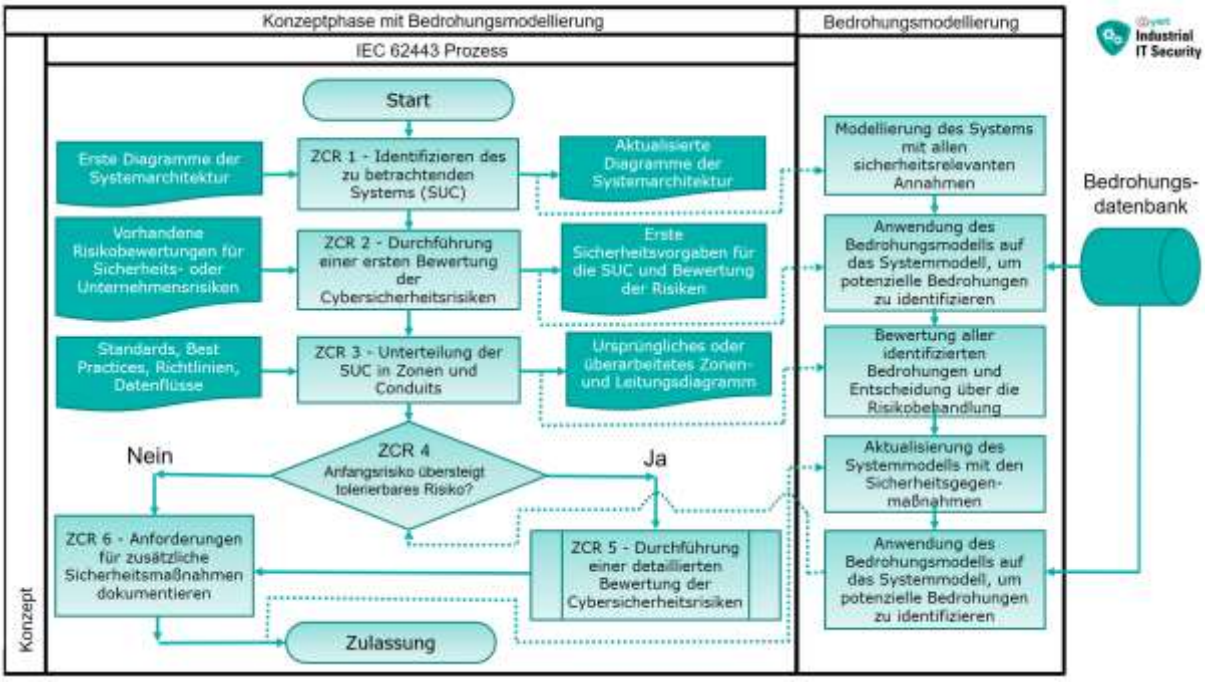

Abbildung 1: *Konzeptphase mit Bedrohungsmodellierung*

In diesem Ablauf werden in jeder Phase die ermittelten Informationen in das Bedrohungsmodell eingegeben. Die Ergebnisse tragen zu einer besseren Risikoanalyse bei.

Wie nun im Einzelnen eine Bedrohungsmodellierung aussieht, erfahren Sie im nächsten Beitrag dieser Serie.

Threat Modeling - Beitrag 12

Bedrohungsanalyse im industriellen Umfeld

In der Literatur werden verschiedene Methoden zur Bedrohungsmodellierung für CPS[5] vorgeschlagen, die unterschiedlichen Anforderungen und Ansätzen von Forschern und Praktikern gerecht werden. Die Wahl einer geeigneten Bedrohungsmodellierungsmethode hängt von der Erfahrung, den Zielen, der Zeit und den Werkzeugen der Beteiligten ab. In der Literatur werden zwar viele Methoden vorgeschlagen, aber nur wenige werden in der Praxis eingesetzt (z. B. **STRIDE**, **LINDDUN**). Im weiteren Verlauf dieser Serie, wird STRIDE eingesetzt. Hier eine kurze Beschreibung dieses Modells.

STRIDE

STRIDE ist ein Kürzel, das erstmals von Microsoft für die Aufzählung von Bedrohungen eingeführt wurde und für **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service und **E**levation of Privilege steht. Die Modellierung von Bedrohungen mit STRIDE erfordert eine Darstellung des betrachteten Systems, die vor allem durch die Verwendung eines Datenfluss-diagramms realisiert wird. STRIDE analysiert die Systemkomponenten im Hinblick auf 6 wichtige Sicherheitseigenschaften (Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung, Autorisierung und Nichtabstreitbarkeit). Die Literatur zeigt jedoch, dass es kein klares Standardverfahren zur Anwendung von STRIDE auf ein CPS gibt. Trotzdem soll STRIDE als Bedrohungmodellierungsmodell hier eingesetzt werden, da es viele Vorteile gegenüber anderen Verfahren bietet.

[5] CPS – Cyber Physical System (dazu gehören auch ICS/IACS)

Tabelle - Die STRIDE-Bedrohungen

Bedrohung	Gefährdetes Eigentum	Definition der Bedrohung	Typische Opfer	Beispiele
Spoofing/Verfälschung	Authentifizierung	Vorgeben, etwas oder jemand anderes zu sein als man selbst	Prozesse, externe Entitäten, Personen	Fälschliche Behauptung, das man Acme.com, winsock.dll, Barack Obama, ein Polizeibeamter oder die Nigerian Anti-Fraud Group sei
Manipulation	Integrität	Etwas auf der Festplatte, in einem Netzwerk oder im Speicher verändern	Datenspeicher, Datenflüsse, Prozesse	Ändern einer Tabellen-kalkulation, der Binärdatei eines wichtigen Programms oder des Inhalts einer Datenbank auf der Festplatte; Ändern, Hinzufügen oder Entfernen von Paketen über ein Netzwerk, entweder lokal oder weit über das Internet hinaus, verdrahtet oder drahtlos; Ändern entweder der Daten, die ein Programm verwendet, oder des laufenden Programms selbst
Repudiation/Ablehnung	Nicht-Abstreitbarkeit	Die Behauptung, dass man etwas nicht getan hat oder nicht verant-wortlich war. Eine Zurückweisung kann wahr oder falsch sein, und die Schlüsselfrage für Systementwickler lautet: Welche Beweise haben Sie?	Prozess	Prozess oder System: "Ich habe nicht auf den großen roten Knopf gedrückt" oder "Ich habe den Ferrari nicht bestellt". Beachten Sie, dass die Ablehnung von Daten hier eine etwas ungewöhnliche Bedrohung darstellt; sie geht über die technische Natur der anderen Bedrohungen für die Geschäftsebene hinaus.
Information Disclosure/ Offenlegung von Informationen	Vertraulichkeit	Weitergabe von Informationen an Personen, die nicht berechtigt sind, sie einzusehen	Prozesse, Datenspeicher, Datenflüsse	Das offensichtlichste Beispiel ist der Zugriff auf Dateien, E-Mails oder Datenbanken, aber die Offenlegung von Informationen kann auch Dateinamen ("Terminierung für John Doe.docx"), Pakete in einem Netzwerk oder den Inhalt des Programm-speichers betreffen.
Denial of Service	Verfügbarkeit	Absorption von Ressourcen, die für die Bereitstellung von Diensten benötigt werden	Prozesse, Datenspeicher, Datenflüsse	Ein Programm, das durch einen Trick dazu gebracht werden kann, seinen gesamten Speicher zu verbrauchen, eine Datei, die die Festplatte füllt, oder so viele Netzwerkverbindungen, dass echter Datenverkehr nicht durchkommen kann
Elevation of Privilege/Erhöhung der Privilegien	Autorisierung	Jemandem gestatten, etwas zu tun, wozu er nicht berechtigt ist	Prozess	Erlaubt einem normalen Benutzer, Code als Administrator auszuführen; erlaubt einer entfernten Person ohne jegliche Berechtigung, Code auszuführen

Mit der Kenntnis des Systems und seiner Einzelheiten können die Kategorien des STRIDE-Frameworks sukzessive auf die Assets und die Schnittstellen angewendet werden

Es ist zu beachten, dass bei der Verwendung von STRIDE zur Suche nach Bedrohungen lediglich die Dinge aufgezählt werden, die schiefgehen könnten. Die genauen Mechanismen, wie es schiefgehen kann, kann später entwickelt werden. Dies kann einfach sein oder eine große Herausforderung darstellen. Es ist auf jeden Fall eine Aufgabe für Sicherheitsexperten, die sich mit realen Angriffen auskennen. Wenn ein möglicher Angriff z.B. die Manipulation eines SPS-Programms wäre, kann jemand sagen: "Nein, das geht nicht, weil...". Daher ist es gut, Schwachstellen und deren Angreifbarkeit genau zu kennen.

Es existieren 2 Varianten von STRIDE. Welche das sind, erfahren Sie im nächsten Beitrag dieser Serie.

Threat Modeling - Beitrag 13

STRIDE-Varianten

STRIDE kann eine sehr nützliche Eselsbrücke bei der Suche nach Bedrohungen sein, aber sie ist **nicht perfekt**.

STRIDE-per-Element

STRIDE-per-Element macht STRIDE präskriptiver, indem es feststellt, dass bestimmte Bedrohungen bei bestimmten Elementen eines Diagramms häufiger vorkommen. So ist es zum Beispiel unwahrscheinlich, dass ein Datenspeicher einen anderen Datenspeicher fälscht. Durch die Konzentration auf eine Reihe von Bedrohungen für jedes Element lassen sich bei diesem Ansatz Bedrohungen leichter finden. Microsoft beispielsweise verwendet Tabelle 3-9 als Kernbestandteil seiner Security Development Lifecycle-Schulung zur Bedrohungsmodellierung.

Tabelle - STRIDE-per-Element

	S	T	R	I	D	E
Externe Entität	X		X			
Prozess	X	X	X	X	X	X
Datenfluss		X		X	X	
Datenspeicher		X	X	X	X	

Anhand dieser Tabelle kann die Bedrohungsanalyse darauf konzentriert werden, wie ein Angreifer z.B. einen Datenfluss manipulieren, Daten auslesen oder den Zugriff darauf verhindern könnte. Wenn beispielsweise Daten über ein Netzwerk wie Ethernet fließen, ist es für jemanden, der an dasselbe Ethernet angeschlossen ist, trivial, den gesamten Inhalt zu lesen, zu verändern oder eine Flut von Paketen zu senden, um eine TCP-Zeitüberschreitung zu verursachen.

Die Bedrohung richtet sich gegen das in der Tabelle aufgeführte Element. Jedes Element ist das Opfer, nicht der Verursacher!

STRIDE-per-interaktion

STRIDE-per-interaction ist ein Ansatz zur Aufzählung von Bedrohungen, der Tupel von (*Ursprung*, *Ziel*, *Interaktion*) berücksichtigt und Bedrohungen gegen diese aufzählt. Ursprünglich bestand ein weiteres Ziel dieses Ansatzes darin, die Anzahl der Dinge, die ein Modellierer berücksichtigen muss, zu reduzieren, aber das hat nicht wie geplant funktioniert.

Im weitere Verlauf dieser Serie wird der Ansatz **STRIDE-per-element** verwendet.

Wie genau eine Bedrohungsmodellierung durchgeführt wird, welche Phasen sie hat, erfahren Sie im nächsten Beitrag dieser Serie.

Threat Modeling - Beitrag 14

Phasen der Bedrohungsmodellierung

Zur Modellierung von Bedrohungen wird eine neunstufige Methodik verwendet.

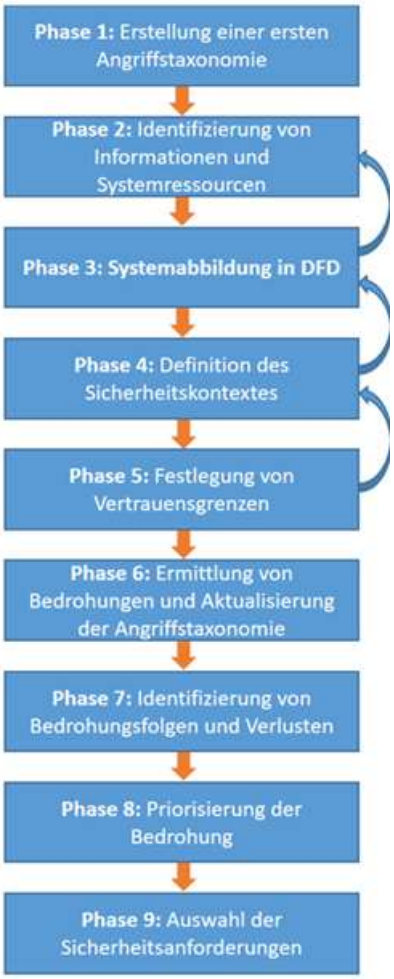

***Abbildung**: Phasen der Bedrohungsmodellierung*

Im Folgenden werden die Phasen genauer beschrieben.

Phase 1 - Erstellung einer anfänglichen Angriffstaxonomie

Die **erste Phase** der vorgeschlagenen Methodik besteht aus der Durchsicht von Literatur und Datenbanken über Angriffe auf ähnliche Systeme (z. B. Energieerzeugung, Krankenhäuser, Produktionsanlagen, usw.) und der Erstellung einer anfänglichen *Angriffstaxonomie*. Dieser Schritt hilft den Cybersicherheitsexperten, sich mit der Zielumgebung und den damit verbundenen Sicherheits-problemen vertraut zu machen.

Phase 2 - Identifizierung von Informationen und Systemressourcen

Das Hauptziel der **zweiten Phase** ist die Identifizierung aller Informations- und Systemwerte, unabhängig davon, ob sie in den Anwendungsbereich der Bedrohungsmodellierung fallen oder nicht. Obwohl es in dieser Phase erforderlich ist, die Systemressourcen im Detail zu identifizieren und zu verstehen, wird ein besonderer Schwerpunkt auf die Auflistung und Kategorisierung der Informationsressourcen gelegt. Dabei ist es auch interessant, welche Kommunikation zwischen welchen Teilsystemen vorhanden ist. Im Vergleich zu einem softwarebasierten System weist ein Automatisierungssystem einige signifikante Unterschiede auf. Viele Automatisierungssysteme arbeiten z.B. mit zwei verschiedenen Informationskategorien, *Steuerung* und *Messung*, die je nach kontrolliertem physikalischem Prozess und zeitlichen Anforderungen (z. B. Echtzeit oder nicht Echtzeit) unterschiedliche Sicherheitsprioritäten haben können.

Das Ziel dieser Phase ist die Erstellung eines ersten *Systemarchitekturdiagramms*, in dem die Systemressourcen identifiziert werden. Anschließend kann das Bedrohungsmodellierungsteam die potenziellen Informationswerte im System diskutieren.

Phase 3 wird im nächsten Beitrag dieser Serie eingehend beschrieben.

Threat Modeling - Beitrag 15

Phase 3 - Systemabbildung in DFD

Ein Datenflussdiagramm (*DFD*) wird in der **dritten Phase** erstellt. DFDs helfen bei der Identifizierung der potenziellen Bedrohungsziele aus der Sicht des Angreifers.

In einem DFD werden Symbole für die grafische Darstellung von Systemen verwendet.

Symbol	Name	Beschreibung
Externe Entität	Externe Entität	Die externe Entitätsform wird verwendet, um jede Entität außerhalb der Anwendung darzustellen, die über einen Einstiegspunkt mit der Anwendung interagiert.
Prozess	Prozess	Das Prozessformat stellt eine Aufgabe dar, die Daten innerhalb der Anwendung verarbeitet. Die Aufgabe kann die Daten verarbeiten oder eine Aktion auf der Grundlage der Daten durchführen.
Datenspeicher	Datenspeicher	Die Form des Datenspeichers wird verwendet, um Orte darzustellen, an denen Daten gespeichert werden. Datenspeicher verändern die Daten nicht, sie speichern sie nur.
Datenfluss	Datenfluss	Die Datenflussform stellt die Datenbewegung innerhalb der Anwendung dar. Die Richtung der Datenbewegung wird durch den Pfeil dargestellt.
Privilegiengrenze	Privilegiengrenze	Die Form der Berechtigungsgrenze (oder Vertrauensgrenze) wird verwendet, um die Änderung der Vertrauensstufen beim Datenfluss durch die Anwendung darzustellen. Grenzen zeigen jeden Ort, an dem sich die Vertrauensstufe ändert.

Abbildung 1: *Symbole eines Datenflussdiagramms*

Hier ein Beispiel für ein DFD für eine Webseite.

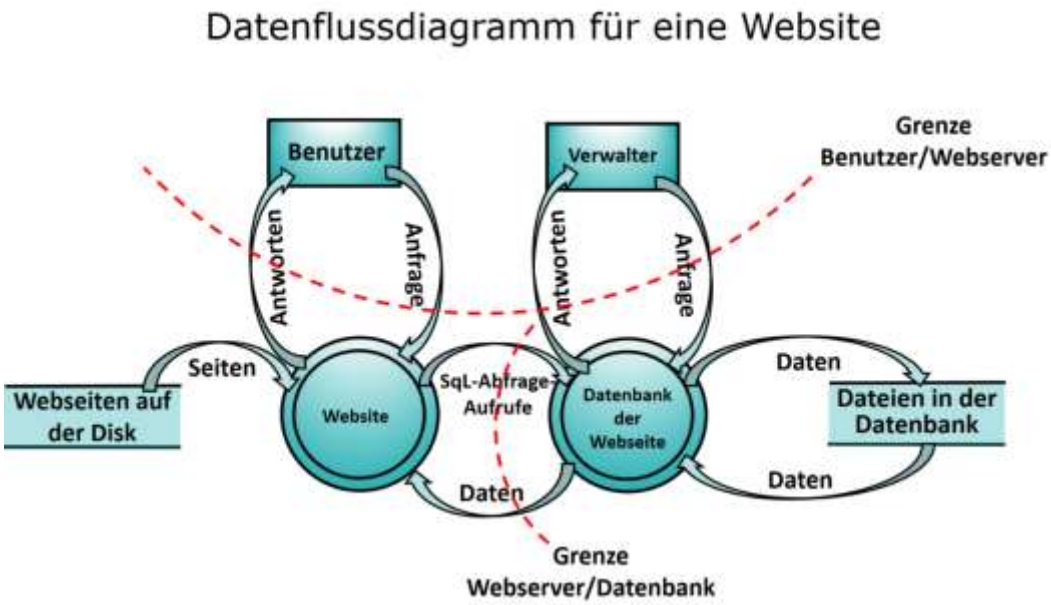

Abbildung 2: *Datenflussdiagramm einer Webseite*

Zur Erstellung solcher DFD's gibt es kostenlose Tools. Eines ist z.B. *Threat Dragon* von **OWASP**.[6]

Wie Bedrohungen in Bedrohungsbäumen klassifiziert werden können, erfahren Sie im nächsten Beitrag dieser Serie.

[6] https://owasp.org/www-project-threat-dragon/

Threat Modeling - Beitrag 16

Bedrohungsbäume

Bedrohungen können als Wurzeln für Bedrohungsbäume weiter klassifiziert werden. Für jedes Bedrohungsziel gibt es einen Baum. Zur Durchführung Bedrohungsanalyse ist ein Bedrohungsbaum sehr hilfreich. Ein Beispiel-Baum wird in der folgenden Abbildung gezeigt.

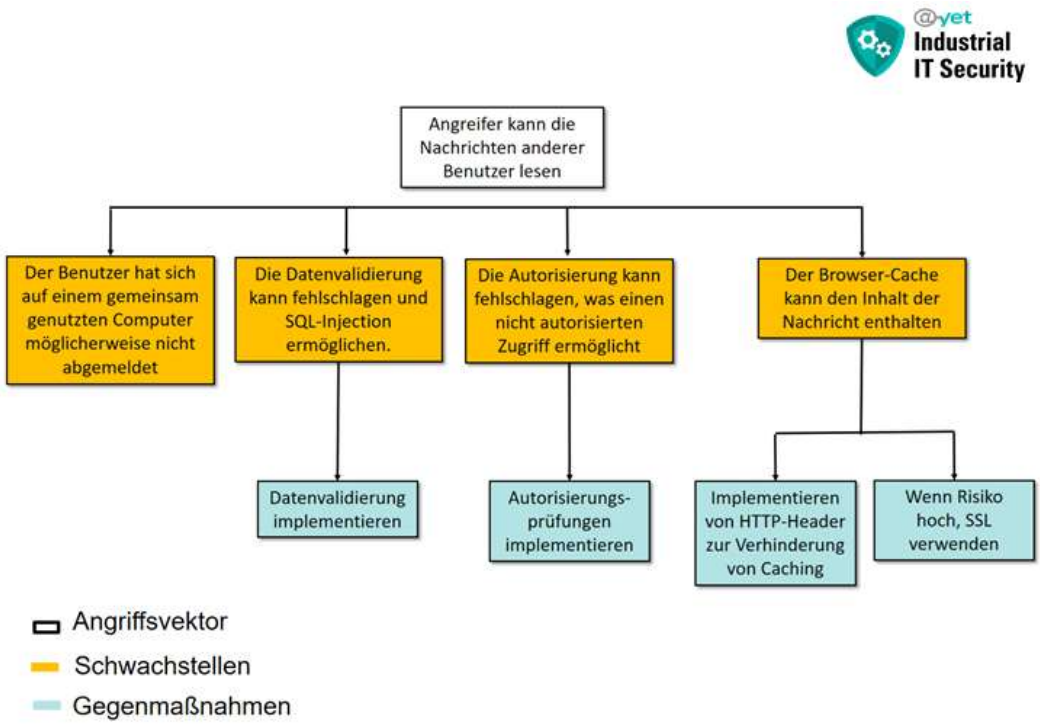

Abbildung: *Beispiel eines Bedrohungsbaums*

Diese Bäume sind nach **STRIDE-pro-Element** geordnet und jeder hat als Wurzelknoten die Realisierung einer Bedrohungsaktion. Jedem Baum folgen eine oder mehrere Tabellen, die den Knoten erklären und Abhilfemaßnahmen für diejenigen, die ein System **entwickeln** und für diejenigen, die es **einsetzen** (*Betrieb*), erörtern. Natürlich werden hier OT-typische Bedrohungsbäume verwendet, die speziell an die betrachtete Anlage anzupassen sind.

An dieser Phase der Systemabbildung sollten **alle** Experten, einschließlich der Systemarchitekten, aktiv an den Diskussionen teilnehmen. Die Verfolgung des Lebenszyklus der Informationsressourcen und die Auswirkungen auf den Informationsfluss sind die wichtigsten Diskussionspunkte in dieser gemeinsamen Arbeit. Auf der anderen Seite ist es wichtig, die physischen Systemkomponenten, die keine Rechenkapazität haben, und die analogen Informationsflüsse zu bestimmen. Obwohl die Bedrohungsmodellierung darauf abzielt, die cyberbezogenen Bedrohungen zu identifizieren, sollen auch die physischen Vermögenswerte und analogen Flüsse im DFD dargestellt werden, da sie für die spezialisierten Systemexperten informativ sein könnten, wenn sie bei der Identifizierung der Bedrohungsfolgen (siehe *Phase 7*) ein Feedback geben.

Wie es mit Phase 4 weitergeht, erfahren Sie im nächsten Beitrag dieser Serie.

Threat Modeling - Beitrag 17

Phase 4 - Definition des Sicherheitskontextes

Die **vierte Phase** wird eingeleitet, nachdem das DFD einen gewissen Reifegrad erreicht hat. In dieser Phase einigt sich das Bedrohungsmodellierungsteam auf die wichtigsten physischen Sicherheitsannahmen, die vertrauenswürdigen Instanzen (z. B. System-administratoren), identifiziert die wichtigsten Bedrohungsakteure, die es auf das System abgesehen haben könnten (z. B. erfahrene Cyberkriminelle), und einigt sich schließlich auf die ausgeschlossenen Angriffe (z. B. Angriffe auf die Lieferkette). Auch hier sind erfahrene Pentester von großem Nutzen.

Phase 5 - Festlegung von Vertrauensgrenzen

Die Ergebnisse der vierten Phase spielen eine Schlüsselrolle in der **fünften Phase**. Zuerst wird eine gute Dokumentation des in Phase 4 ermittelten Sicherheitskontextes erstellt, gefolgt von einer dokumentierten Begründung für die Wahl der Vertrauensgrenzen. Eine solche Dokumentation erleichtert die erneute Prüfung von Grenzentscheidungen im Falle von Systemänderungen oder der Identifizierung neuer Sicherheitskontexte. In einigen Fällen kann es erforderlich sein, von der vierten und fünften Phase zur zweiten und dritten Phase zurückzukehren, um die Bestandslisten und das DFD zu überarbeiten. Alle Teammitglieder sollten bei den Diskussionen dieser Phasen zusammenarbeiten und sich über die Ergebnisse einigen.

Phase 6 - Ermittlung von Bedrohungen

Die **sechste Phase** ist hauptsächlich der Ermittlung der Bedrohungen auf der Grundlage des **STRIDE-pro-Element-Ansatzes** gewidmet, bei dem jede Komponente in den DFDs einzeln analysiert wird (eine alternative Methode, **STRIDE-per-interaction**, konzentriert sich auf die Informationsflüsse, die die Vertrauensgrenzen überschreiten).

Die Verwendung des Optimierungsansatzes **STRIDE-pro-Element** ermöglicht es dem Bedrohungs-modellierungsteam, die Situationen der einzelnen Geräte in Bezug auf den physischen Zugriff und die Cyber-Folgen zu berücksichtigen. **Tabelle 1** wird für die Zuordnung der DFD-Elemente zu den Bedrohungskategorien von STRIDE verwendet.

Tabelle - Anwendbare Bedrohungen für DFD-Elemente

DFD Element	S	T	R	I	D	E
Entität	✓		✓			
Datenfluss		✓		✓	✓	
Datenspeicher		✓	✓	✓	✓	
Prozess	✓	✓	✓	✓	✓	✓

Nun müssen Angriffe, die zu den relevanten Bedrohungen passen, aufgelistet werden.

Wie in Phase 6 die relevanten Bedrohungen ermittelt werden, erfahren Sie im nächsten Beitrag.

Threat Modeling - Beitrag 18

Ermittlung von Bedrohungen

Zur Ermittlung von Bedrohungen werden die ermittelten *Angriffe* und die *Informationswerte* in die Analyse einbezogen.

Reihenfolge der Bedrohungserhebung:

- Es wird ein DFD-Element ausgewählt
- Die Praktiker identifizieren die relevanten Informationsbestände
- Die Bedrohungskategorie (S T R I D E) wird ausgewählt
- Die Angriffe werden auf die anwendbaren Angriffstypen angewendet

Jede für ein bestimmtes DFD-Element erstellte Bedrohungsdefinition hat hauptsächlich drei gemeinsame Komponenten:

(1) einen Vorbedingungs-Angriffszustand, der aus der Liste der Angriffe abgeleitet wird

(2) den/die möglichen Angriffsvektor(en) für diese Bedrohung

(3) die betroffenen Informationsgüter.

Um die Integration zwischen **STRIDE** und den vorgeschlagenen Angriffstypen zu erleichtern, wird die Zuordnung von STRIDE zu den ersten beiden Komponenten der vorgeschlagenen Bedrohungsdefinition (*Angriffsvorbedingung* und *mögliche Angriffsvektoren*) auf der Grundlage der Taxonomie zusammengefasst.

Die Diskussionen über die Bedrohungserhebung finden (meist) unter den Cybersicherheitsexperten statt. Die Zwischen- und Endergebnisse werden jedoch mit den anderen Experten geteilt, um weitere Meinungen einzuholen. Im Vergleich zu den vorangegangenen Phasen (z. B. *Identifizierung von Vermögenswerten* und *Systemabbildung*) ist der Beitrag des Systemeigentümers und der Systemarchitekten relativ gering. Diese Phase wird durch eine Überprüfung und Aktualisierung der Angriffstaxonomie abgeschlossen.

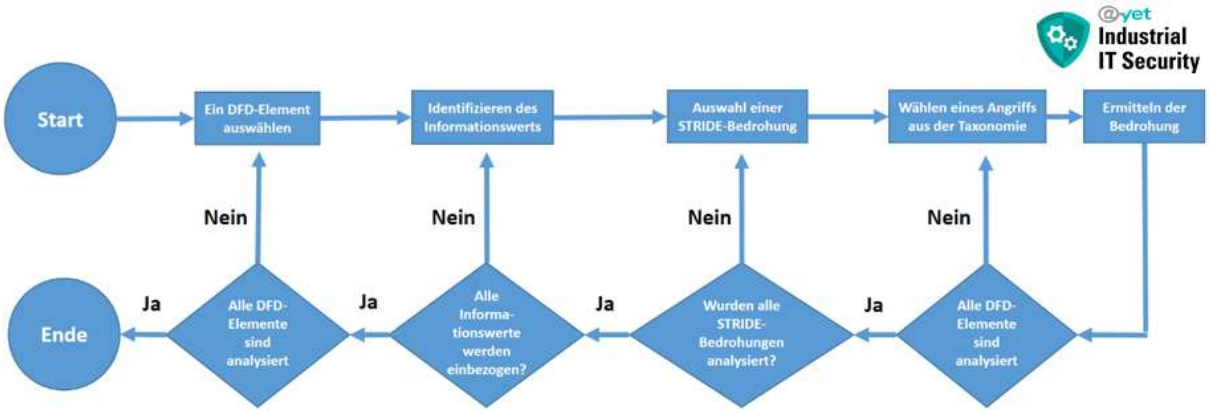

Abbildung: *Verfahren zur Ermittlung von Bedrohungen.*

Mit der Phase 7 geht es im nächsten Beitrag dieser Serie weiter.

Threat Modeling - Beitrag 19

Phase 7 - Identifizierung von Bedrohungsfolgen und Verlusten

Die **siebte Phase** wird von den Systemexperten unter der Anleitung der Cybersicherheitsexperten durchgeführt. Das Erfassen der Konsequenzen der Bedrohungen ist ein erheblicher Aufwand zur Bewertung und Einstufung der Bedrohungen. Das Team sollte jede der ermittelten Bedrohungen durchgehen und die Folgen der Bedrohung sowie die damit verbundenen potenziellen materiellen und immateriellen Verluste ermitteln. Hier sind Erfahrungen von Pentestern und IT-Forensikern Gold wert.

Die Ergebnisse des Bedrohungsmodellierungsprozesses sollten den Systementwicklern und allen anderen Beteiligten eine Liste von Sicherheitsanforderungen liefern, die auf das System angewendet werden können, um die ermittelten Schwachstellen zu mindern. Um dies zu erreichen, ist es sinnvoll, die Bedrohungen auf der Grundlage ihrer Folgen und potenziellen Verluste zu priorisieren, da diese Informationen den Beteiligten bei der Auswahl der Sicherheitsanforderungen helfen können.

Phase 8 - Priorisierung der Bedrohungen

Das Erfassen der Konsequenzen der Bedrohungen ist ein erheblicher Aufwand zur Bewertung und Einstufung der Bedrohungen. In der siebten Phase wurden die möglichen Folgen jeder festgestellten Bedrohung ermittelt. Diese könnten zur Beurteilung der Priorität verwendet werden.

Weiter können auch Schwachstellenbeurteilungen (z.B. CVSS[7]) eingesetzt werden, um festzulegen, wie kritisch eine Bedrohung ist.

Welche Sicherheitsanforderungen von der IEC 62443 bezüglich der ermittelten Bedrohungen und des ausgewählten Sicherheitslevels gefordert werden, erfahren Sie im nächsten Beitrag dieser Serie.

[7] CVSS – Common Vulnerability Scoring System; www.first.org/cvss/

Threat Modeling - Beitrag 20

Phase 9 - Auswahl der Sicherheitsanforderungen

Eine Schwachstelle kann durch die Implementierung einer Gegenmaßnahme entschärft werden. Der Zweck der Identifizierung von Gegenmaßnahmen besteht darin, festzustellen, ob es irgendeine Art von Schutzmaßnahme (z.B. *Sicherheitskontrolle*, *Richtlinien*) gibt, die verhindern kann, dass eine Bedrohung realisiert wird.

Für die benötigten Gegenmaßnahmen zur Risikominderung in einer Automatisierungsanlage, werden die Anforderungen des **IEC 62443-3-3** verwendet. Abhängig vom gewählten *Sicherheitslevel-Target*[8] sind hier die notwendigen Anforderungen beschrieben.

So könnte z.B. eine Bedrohung beim Login für einen SCADA-Server ermittelt worden sein. Um hier Gegenmaßnahmen einzubauen, kann die grundlegende Anforderung **FR1.1** verwendet werden. Abhängig vom gewählten Sicherheitslevel werden hier entsprechende Anforderungen gestellt. Wurde z.B. **SL2** ausgewählt, sind die Maßnahmen **SR1.1**, **SR1.1 RE[9] 1**, und **SR1.1 RE2** umzusetzen.

***Tabelle** – Anforderungen für unterschiedliche Sicherheitslevel*

Tabelle – Abbildung von SR und RE auf die FR 1.1 für SL 1– 4					
SR und RE		**SL 1**	**SL 2**	**SL 3**	**SL 4**
FR 1 – Identifizierung und Authentifizierung (IAC)					
SR 1.1 – Identifizierung und Authentifizierung von menschlichen Nutzern		X	X	X	X
SR 1.1 RE 1 – Eindeutige Identifizierung und Authentifizierung			X	X	X
SR 1.1 RE 2 – Multifaktor-Authenti-fizierung über nicht vertrauenswürdige Netze				X	X
SR 1.1 RE 3 – Multifaktor-Authentifizierung über alle Netze					X

Wie die Risikobewältigung aussieht, erfahren Sie im nächsten Beitrag dieser Serie.

[8] zu erreichender Sicherheitslevel nach IEC62443

[9] RE: Requirement Enhancement (*weitergehende Anforderung*)

Threat Modeling - Beitrag 21

Es gibt verschiedene Möglichkeiten, das Risiko zu bewältigen:

- **Akzeptieren**: entscheiden, dass die Auswirkungen auf das Geschäft akzeptabel sind
- **Beseitigen**: Komponenten entfernen, die die Schwachstelle ermöglichen
- **Abschwächen**: Hinzufügen von Prüfungen oder Kontrollen, die die Auswirkungen des Risikos bzw. die Wahrscheinlichkeit seines Auftretens verringern

STRIDE-Bedrohungs- und Entschärfungstechniken

Mögliche Gegenmaßnahmen von STRIDE Bedrohung sind in der folgenden Tabelle aufgeführt.

***Tabelle** - Gegenmaßnahmen von STRIDE Bedrohungen*

Art der Bedrohung	Techniken zur Schadensbegrenzung
Identität fälschen	1. Angemessene Authentifizierung 2. Schutz der geheimen Daten 3. Keine Geheimnisse speichern
Manipulation von Daten	1. Angemessene Autorisierung 2. Hashes 3. MACs 4. Digitale Signaturen 5. Manipulationssichere Protokolle
Ablehnung	1. Digitale Unterschriften 2. Zeitstempel 3. Prüfpfade
Offenlegung von Informationen	1. Autorisierung 2. Datenschutz-erweiterte Protokolle 3. Verschlüsselung 4. Schutz von Geheimnissen 5. Keine Geheimnisse speichern
Denial of Service	1. Angemessene Authentifizierung 2. Angemessene Autorisierung 3. Filterung 4. Drosselung 5. Qualität der Dienstleistung
Ausdehnung von Privilegien	1. Betrieb mit geringsten Privilegien

In der Norm **DIN CEN ISO/TR 22100-4**[10] (Leitlinien für Maschinenhersteller zur Berücksichtigung der damit verbundenen IT-Sicherheits- (Cybersicherheits-) Aspekte werden Beispiele[11] für risikomindernde Maßnahmen, die Einfluss auf die Sicherheit von Maschinen haben können,

[10] Deutsche Fassung CEN ISO/TR 22100-4:2020
[11] Abschnitt 9 Tabelle 3 - Beispiele für risikomindernde (-verringernde) Maßnahmen zur Vermeidung/Begrenzung von Bedrohungen der IT-Sicherheit, die Einfluss auf die Sicherheit von Maschinen haben können

tabellarisch aufgeführt. Dabei wird die Rolle (Maschinenhersteller, Integrator, Endbenutzer), die die Maßnahme durchführen sollte, mit benannt. So kann z.B. die risikomindernde Maßnahme „Bereitstellung eines IT-Systems mit risikomindernden (-verringernden) Maßnahmen (z. B. Firewalls, Antivirentools)“ von allen drei Rollen durchgeführt werden, während die „Begrenzung der Benutzerrechte des IT-Systems nur auf diejenigen, die für die Rolle jeder Person erforderlich sind“ nur vom Endbenutzer durchgeführt werden kann. Die angegebenen Beispiele geben eine gute Übersicht über mögliche Maßnahmen.

Sobald die Bedrohungen und die entsprechenden Gegenmaßnahmen ermittelt sind, kann ein Bedrohungsprofil mit den folgenden Kriterien erstellt werden:

- **Nicht entschärfte Bedrohungen**:
  - Bedrohungen, für die es keine Gegenmaßnahmen gibt
  - Schwachstellen die vollständig ausgenutzt werden können und Auswirkungen haben
- **Teilweise entschärfte Bedrohungen**:
  - können durch eine oder mehrere Gegenmaßnahmen teilweise gemildert werden
  - nur teilweise ausnutzbar mit begrenzter Auswirkung
- **Vollständig abgeschwächte Bedrohungen**:
  - verfügen über geeignete Gegenmaßnahmen und stellen keine Schwachstellen dar

Im nächsten und letzten Teil dieser Beitragsserie wird ein Fazit zur Bedrohungsmodellierung im OT Umfeld gezogen.

Threat Modeling - Beitrag 21

Fazit

Die Bedrohungsmodellierung ist ein kreativer Prozess, der sehr viel Erfahrung und an mancher Stelle auch tiefes technisches Wissen und Verständnis erfordert!

Mit einer Bedrohungsmodellierung können mögliche Angriffe auf ein Automatisierungssystem sehr gut vorhergesagt und mögliche Schwachstellen ermittelt werden. Als Ergebnis wird eine Dokumentation erstellt, die es erlaubt, notwendige Gegenmaßnahmen zu finden. Weiterhin kann mit dem gezeigten Vorgehen regelmäßig eine erneute Analyse durchgeführt. Denn, wie allgemein bekannt: Security ist eine **Momentaufnahme**! Was heute sicher ist, kann morgen unsicher sein. Daher sollte eine Bedrohungsmodellierung regelmäßig aktualisiert werden.

Die genaue Kenntnis von möglichen Angriffen führt auch dazu, dass Investitionen in die Verteidigung punktgenau eingesetzt werden können. Das kann zu Einsparungen führen, die die Investition in eine Bedrohungsmodellierung auch wieder lukrativ machen kann.

Neben den Details zu möglichen Angriffen wird auch eine detaillierte Dokumentation zur untersuchten Anlage erstellt. Dabei werden die Komponenten und deren Kommunikation mit anderen Komponenten aufgelistet. Diese Dokumentation kann auch im Falle eines erfolgreichen Angriffs gegen die Automatisierungsanlage bei einer Forensik hilfreich sein, zu kürzeren Stillstandzeiten führen, aber auch die Forensik selber verkürzen. All das führt zu geringeren Kosten/Verlusten.

Aber auch die Auseinandersetzung des Bedien-, Administrations- und Wartungspersonals mit den möglichen Angriffen sensibilisiert den Umgang mit Security. Hier wird Awareness geschaffen wie es oft nur bei zugeschnittenen Schulungen der Fall ist. Aber neben der Awareness erkennen IT- und OT-Personal, dass es eine gemeinsame Aufgabe ist, das Ziel zu erreichen. Es werden die Probleme der jeweils anderen Gruppe erkannt und erfahren und so ist eine Kommunikation sehr viel einfacher.

Bei Fragen zum Thema *Threat Modeling* senden Sie bitte eine Email an info@add-yet-iis.de