Die Entdeckung der Bedrohung kes 01/2024

FMEA-EINSATZ ZUR BESSEREN BEWERTUNG VON INFORMATIONSSICHERHEITS-RISIKEN

Die Kernaufgabe der Informationssicherheit ist es, mögliche Bedrohungen und passende Schutzmaßnahmen in ein beherrschbares Gleichgewicht zu bringen. Hierbei unterliegt Beherrschbarkeit üblicherweise einer Risikoabwägung, in der die Erkennung von Bedrohungen derzeit keine Rolle spielt. Unser Autor schlägt vor, mithilfe der „Failure Mode and Effects Analysis" (FMEA) das Informationssicherheits-Management um das Element der Entdeckungswahrscheinlichkeit zu erweitern. Hierdurch erhalten sowohl Möglichkeiten zur Angriffserkennung als auch passende Hindernisse eine hinreichende Würdigung.

Bedrohungen sind der Treibstoff der Informationssicherheit. Als Kehrseite der Digitalisierung der Welt hat der Schutz von Systemen und Daten einen hohen, für KRITIS-Segmente sogar essenziellen Stellenwert erlangt. Aufgrund der besonderen gesellschaftlichen Bedeutung hat das „Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (BSIG 2.0) für diese Segmente besondere Anforderungen und Verpflichtungen definiert. Eine wesentliche Neuerung sind dabei Einführung und Betrieb von „Systemen zur Angriffserkennung", mit denen eine proaktive und ex ante Erkennung von Cyberangriffen ermöglicht und eine Schadensreduktion oder gar -vermeidung unterstützt werden soll [1]. Dazu sollen Informationen aus dem laufenden Betrieb erfasst und mit dem Fokus auf Bedrohungen ausgewertet werden.

Die Erfüllung dieser Anforderungen haben Betreiber kritischer Infrastrukturen regelmäßig alle zwei Jahre dem BSI gegenüber nachzuweisen. Wie bei allen Maßnahmen zur Informationssicherheit sind auch hier Ausprägung und Umfang der Maßnahmen risikoorientiert vorzunehmen – dies wird jedoch im Gesetz sowie in der Orientierungshilfe des BSI zum Einsatz von SzA (OH SzA, [1]) maximal indirekt adressiert.

Systeme zur Angriffserkennung

Betreiber kritischer Infrastrukturen sind verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten und Prozesse zu treffen. Hierzu zählen mit den Änderungen des IT-Sicherheitsgesetzes von 2021 nun auch der Einsatz von Systemen zur Angriffserkennung (SzA). Entsprechend der Definition in § 2 BSIG sind dies „durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen“. Fokussiert wird also nicht auf ein technisches System, sondern auf manuelle und gegebenenfalls automatisierte Prozesse, die durch Technik unterstützt werden. Zielsetzungen sind „fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen“. Im Sinne von Informationssicherheitssystemen stellen SzA als Prozesse einen Teil der Managementaufgaben dar. Demzufolge orientieren sich Anforderungen an SzA am IT-Grundschutz, der nach Auffassung des BSI den „Stand der Technik“ darstellt.

Zur Erkennung von Angriffen sind „geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch zu erfassen und auszuwerten“. Hieraus ergeben sich für die Umsetzung, den Betrieb und schließlich auch den Nachweis sowohl Anforderungen als auch Fragen zu Wirksamkeit und Schutzniveau von SzA: Aus dem laufenden Betrieb sollen kontinuierlich geeignete Parameter und Merkmale erfasst werden – welche Parameter und Merkmale sind geeignet oder relevant, um Angriffe zu erkennen und welche Betriebsdaten erforderlich (d. h. zu erheben), um diese zu erfassen? Die Antworten hängen einerseits von der Definition des Begriffs „Angriff“ sowie der Zielsetzung der Erkennung ab – andererseits auch von den Merkmalen und dem Wissen über Mechanismen und Abläufen derselben.

Das BSI-Grundschutz-Kompendium definiert Angriff als „eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen beziehungsweise einen Dritten zu schädigen. Ein Angriff kann auch im Auftrag von Dritten, die sich

Vorteile verschaffen wollen, erfolgen“. Diese recht allgemeine Definition von Angriffen ist für die Festlegung der zu erfassenden Daten nicht sehr hilfreich.

Ausgehend von der Zielsetzung, Bedrohungen zu identifizieren ist ein Rückgriff auf auslösende Gefährdungen oder Gefährdungsarten besser geeignet: Zu nennen wären etwa Missbrauch von Berechtigungen, Verhinderung oder Überlastung von Diensten (DoS) oder auch das Einspielen manipulierter Daten (z. B. manipulierte Update-Daten). Hierzu passende Parameter und Merkmale zur Erkennung wären beispielsweise unerlaubte Zugriffe/Zugriffsversuche, unerlaubte Berechtigungsänderungen, ungewöhnliche Dienste-/Servicenutzungen und andere.

Als weiterer Schritt ist es daraufhin notwendig, Systeme sowie Protokolldaten und Protokollierungsvorgänge zu bestimmen, mit denen die gewünschten Daten erhoben werden, durch die diese Parameter und Merkmale entweder direkt oder indirekt erkennbar sind. Hierbei sind keineswegs nur die Daten kritischer Systeme an sich zu erheben, sondern auch diejenigen, die für den operativen und administrativen Betrieb der Systeme erforderlich sind.

Betriebliche Daten sind kontinuierlich auszuwerten, was bedeutet, dass man die Betriebsdaten auf das Vorliegen der identifizierten Parameter und Merkmale untersuchen muss. Solche Analysen können in einer großen Bandbreite von simplem Abgleichen à la Virensignaturen bis hin zu komplexen Verknüpfungen von Daten mittels logischer Schlussfolgerungen gestaltet oder sogar erforderlich werden. Während Ersteres noch automatisiert erfolgen kann, ist Letzteres (noch) manuell durchzuführen.

Die Definition von SzA im BSIG geht von einem „Abgleich mit Informationen und technischen Mustern“ aus. Ohne Anspruch auf Vollständigkeit umfasst dies Identifikations-/Authentifizierungsprüfungen als Zählung von Anmeldeversuchen oder Bewertung der Geolokation von Authentifizierungsanfragen, Anomalieerkennung auf Netzwerk-, Host-, Protokoll-, Anwendungs-, Kommunikations- oder Betriebssystemebene, signaturbasierte Abgleiche und Attack-Pattern-

Abgleiche. Weitere Kennzeichen möglicher Anomalien sind beispielsweise in der BSI-Empfehlung „Monitoring und Anomalieerkennungen in Produktionsnetzwerken“ [2] dargestellt.

Unter kontinuierlicher Auswertung versteht das BSI in der OH SzA auch die nachträgliche Erkennung von Bedrohungen. Ohne Definition, wie und über welchen Zeitraum eine Aufbewahrung und wiederkehrende Prüfung der Protokoll- und Protokollierungsdaten zu erfolgen hat und ob dies dann ausreichend ist, wird hiermit zweierlei manifestiert: Signaturen und signaturbasierte Detektionssysteme haben die grundlegende Schwäche, dass sie nicht all-aktuell sind und dass – abhängig von Prozessen zur Signaturaktualisierung – Bedrohungserkennungen somit zeitbehaftet sind. Dies begründet dann auch, die Klassifizierung erreichbarer Schutzniveaus durch derartige Systeme nicht allzu hoch anzusetzen.

Zur vollständigen Umsetzung der Anforderungen sind mit der Auswertung passende Prozesse zur Reaktion auf identifizierte Bedrohungen, eine kontinuierliche Anpassung an neue Bedrohungskategorien sowie eine ständige Verbesserung der Erkennungsrate verbunden. Festzuhalten ist ebenfalls, dass das „System zur Angriffserkennung“ zu einem „bedrohungszentrierten Teil“ des Informationssicherheits-Managementsystems (ISMS) mutiert und sowohl dynamische als auch komplexe Bedrohungslagen behandelt.

Erkennung als wesentliches Merkmal

Die Erkennung ist ein wesentliches Merkmal, genauer: eine wesentliche Anforderung der SzA. Sie lässt sich auf unterschiedliche Arten umsetzen und dies bewirkt – wie schon angedeutet – sehr unterschiedliche Schwierigkeitsgrade, die durch die im Folgenden beschriebenen wesentlichen Aspekte gekennzeichnet werden können.

Zunächst gilt es, die Zielsetzungen und Anforderungen zu definieren. Abhängig hiervon sind die erforderlichen beziehungsweise systemtechnisch verfügbaren Daten zu definieren, aus denen man Bedrohungen „herauslesen“ kann. Hierzu gilt es schon zu unterscheiden, ob Bedrohungen aus einzelnen Datensätzen beziehungsweise Protokollierungsereignissen erkennbar sind oder ob Verknüpfungen von Daten und Ereignissen vorgenommen werden müssen. Solche Verknüpfungen

sind dann wiederum mit dem Wissen über Angriffsmechanismen verbunden – sei es über bestehende oder auch „vorstellbare“ Mechanismen, um abweichende Angriffsszenarien einordnen zu können.

Unabhängig davon, ob eine Erkennung automatisiert oder manuell durchgeführt wird, ist eine Bewusstheit über die Grenzen der Erkennung erforderlich. Diese kann sich im einfachsten und gegebenenfalls „heilbaren“ Fall schon als Zeitfaktor darstellen, etwa wenn Signaturen oder Indicators of Compromise / Attack (IoC/IoA) für automatisierte Prozesse nicht zeitnah genug zur Verfügung stehen.

Andererseits ist die Korrelation schwellwertbezogener Ereignismeldungen – wie fehlgeschlagene Anmeldeversuche oder übertragenes Datenvolumen – immer vom definierten Zeitraum der Bewertung abhängig: Auch das Wissen sowie die Wissensvermittlung und der Wissensempfang über neue Angriffsmethoden und/oder Angriffswerkzeuge sind unter Umständen mit einem Zeitversatz und damit einem höheren Bedrohungspotenzial versehen. Weiterhin sind ebenfalls allzu menschliche Denkansätze oder -hindernisse gegeben, die eine fehlerhafte Bewertung von Bedrohungssituationen eröffnen. Und schließlich muss eingestanden werden, dass ein Vorhersehen von Angriffsmethoden schlichtweg nicht umfassend genug sein kann – auch wenn dies durch Schulung und intensivem Austausch mit Peer-Gruppen angestrebt wird.

Festzuhalten ist, dass besonders eine erfolgreiche Anomalieerkennung einerseits umfangreiche Erhebungen des „Normalzustands“ und andererseits einen permanenten Abgleich mit Betriebsprozessen im Sinne der In- oder Außerbetriebnahme von Systemen, Netzwerkverbindungen, Anwendungen/Protokollen et cetera erfordern. Der Effekt, dass für eine Anomalieerkennung kein exaktes Wissen zu Angriffsstrukturen und IoC/IoA erforderlich ist, wird gegebenenfalls durch viele falschnegative Alarmmeldungen zunichtegemacht.

Festzuhalten ist somit auch, dass die Erkennung an sich ein komplexer Vorgang ist, der von beeinflussbaren und nicht beeinflussbaren Faktoren sowie einer gegenseitigen Beeinflussung der

Parameter und Merkmale abhängt und daher im Rahmen von Risikoanalysen berücksichtigt werden sollte.

FMEA-Einsatz

Die „Failure Mode and Effects Analysis“ (FMEA – deutsch: Fehlermöglichkeits- und Einflussanalyse) ist eine strukturierte Methode zur Ermittlung und Bewertung von Fehlermöglichkeiten. Als qualitative Methode ist dieses Verfahren in Design- und Entwicklungsphasen sowie zur Prozess- und Serviceanalyse mit der Zielsetzung der frühzeitigen Erfassung, Bewertung und Handlungspriorisierung von Risiken auf Systemfehler etabliert.

Der FMEA-Ursprung ist eng verbunden mit dem Qualitätsmerkmal „Safety“ – die ursprüngliche Zielsetzung war es, mögliche (System-) Fehler bereits vor einer Nutzung des Systems zu erkennen und behandeln. Dies sollte einerseits eine Erhöhung der Zuverlässigkeit bewirken, hat aber andererseits auch zu einer Reduzierung des Aufwands zur Mängelbehebung von Produkten und Leistungen geführt [3]. Begründet und stark verbreitet sind FMEA-Methoden im Bereich der Luft- und Raumfahrt sowie Automobiltechnik, also dort, wo eine Gefahr Einfluss auf Leib und Leben hat. Aufgrund ihrer strukturierten und risikoorientierten Vorgehensweise ist eine Anwendung im Bereich Informationssicherheit grundlegend gegeben, jedoch in der Praxis (noch) nicht verbreitet.

Zusätzliches Kriterium: Entdeckungswahrscheinlichkeit

Das Qualitätssystem FMEA bewertet im Rahmen einer Risikobewertung Systemfehler sowie deren Auftretens- und Schweregrad. Während diese Kriterien auch aus anderen Risikokontexten bekannt sind, gibt es im FMEA-Kontext zusätzlich noch das Einflusskriterium „Entdeckungswahrscheinlichkeit“, das die Wahrscheinlichkeit ausdrückt, mit der sich ein möglicher Fehler rechtzeitig erkennen lässt.

Mittels dieser drei Kriterien – Schweregrad, Auftreten und Erkennung – wird eine Risikobewertung durchgeführt, die zur Steuerung von Maßnahmen und Ressourcen zur Minderung von Fehlern dient. Nach neuerer Interpretation wird diese Bewertung nicht länger mittels Multiplikation von jeweils 10-stelligen Bewertungsstufen zu einer sogenannten Risiko-Prioritäts-Nummer (RPN) durchgeführt.

Stattdessen wird eine Kategorisierung in wenigen Stufen diskutiert, die zu einer Handlungspriorität (Action-Priority) verknüpft werden.

Festzuhalten ist, dass die FMEA-Methode von einem möglichen Systemfehler aus „rückwärts“ bis auf Funktionen und Komponenten vorgeht.

Einordnung von Sicherheitskriterien

Aus allgemeiner Sicht und gerade im Kontext der SzA stellt sich die Frage, ob die FMEA-Methode in der Informationssicherheit vorteilhaft anwendbar ist. Hierzu ist zunächst eine Interpretation (Transformation) der verwendeten FMEA-Kriterien mit Sicherheitskriterien vorzunehmen.
Das Auftreten eines Fehlers und damit die Auftretenswahrscheinlichkeit kann sinnvollerweise auf die Bedrohung, genauer auf das Bedrohungspotenzial übertragen werden. Auch wenn man in Risikobetrachtungen der Informationssicherheit häufig eine Eintrittswahrscheinlichkeit verwendet, ist dies nach Auffassung des Autors für SzA nicht zielführend: Gerade fortschrittliche Bedrohungen wie Advanced Persistent Threats (APTs) haben eben keine hohe Eintrittswahrscheinlichkeit, implizieren aber ein hohes Risiko für die Organisation, sofern sie nicht rechtzeitig erkannt werden.

Der bei FMEA verwendete zweite Begriff des Schweregrads drückt den Einfluss auf die Funktionsfähigkeit des Systems aus. Hierfür wird in der Informationssicherheit in der Regel mit Begriffen wie Schadenshöhe oder Schadensauswirkungen operiert. Um hier ein höheres Augenmerk auf die Auswirkung zu legen, wird dies nachfolgend als „Impact“ oder „Value“ bezeichnet.

Die Entdeckungswahrscheinlichkeit ist, wie angesprochen, bislang nicht Bestandteil von standardisierten Risikobewertungen der Informationssicherheit. Gerade der proaktive Ansatz, Risiken aufzudecken, bevor sie eintreten, erscheint jedoch im Rahmen der SzA-Prozesse hilfreich zu sein. Wie schon im Terminus SzA verankert, liegt der Fokus auf der Erkennung von Angriffen. Die mit der Gestaltung und dem Betrieb von SzA verbundenen technischen und/oder organisatorischen Erkennungslücken sind jedoch ebenfalls relevant für den Schutz kritischer Systeme.

Die Verknüpfung der drei Kriterien zur Risikobestimmung erfolgt in FMEA heute nicht mehr durch Multiplikation von Einstufungswerten, sondern durch eine qualitative Verknüpfung – dieser qualitative Ansatz ist auch in der Informationssicherheit gebräuchlich.

Risikobestimmung mit Entdeckungswahrscheinlichkeit in der Informationssicherheit

Eine zu geringe Kontextabhängigkeit von Risikobewertungen in der Informationssicherheit ist eine der größten Unsicherheiten und Fußangeln bei der Bewertung von Auswirkungen beziehungsweise Definition von Maßnahmen. In der Regel erfolgt eine Risikobewertung anhand der Parameter Eintrittswahrscheinlichkeit und Schadenshöhe als eine generelle Einschätzung des Auftretens eines (Gefährdungs-) Ereignisses beziehungsweise dessen Auswirkungen. Weniger angewandt ist die Verknüpfung von Sub-Kriterien wie die „Errechnung (Addition)“ beim Cyber-Sicherheits-Check der Allianz für Cyber Security (ACS) [4]. Auch die Definition geeigneter Maßnahmen zur Risikobehandlung geht in der Regel von einer isolierten Wirksamkeit aus und betrachtet die Voraussetzungen zu einer maximalen Effizienz der Maßnahmen zu wenig.
Diese Vorgehensweise bietet, kombiniert mit einer nicht-fundierbaren Kosten-Nutzen-Berechnung, an sich schon genügend Spielraum für Diskussionen zur korrekten Risikoeinschätzung. Auch die OH SzA konstatiert, dass „geforderte Sicherheitsvorkehrungen in ihrer konkreten Umsetzung Freiheiten zulassen, innerhalb dessen gleichwertige und individuelle Alternativen, unter Berücksichtigung ihrer Angemessenheit, möglich sind“.

Die Einführung und Verwendung der Entdeckungswahrscheinlichkeit kann dabei helfen, die Priorisierung von Maßnahmen sowie Prozesse zu einem SzA zu unterstützen. Damit lässt sich einerseits eine Bewertungsgrundlage im Nachweisverfahren schaffen, andererseits ist gegebenenfalls eine Verknüpfung mit dem vom BSI dargestellten Umsetzungsgradmodell möglich.

Die Integration der Entdeckungswahrscheinlichkeit als drittes Kriterium in Risikobewertungen ist (unabhängig von der Anzahl der Stufen/Kategorisierungen) in den gängigen zweidimensionalen Risikomatrizen nicht möglich. Daher wird im Folgenden auf eine Tabellenform zurückgegriffen, die an die Form der qualitativen FMEA-Tabelle nach Werdich [5] angelehnt ist und auf Aspekte der

Informationssicherheit angepasst wurde. Wie üblich gilt, dass eine höhere Stufe ein höheres Bedrohungspotenzial und einen größeren Einfluss beziehungsweise höheres Ausmaß kennzeichnet. Dies gilt auch für die Entdeckungswahrscheinlichkeit, die durch eine Abstufung von technischen und/oder organisatorischem Detektionsaufwand gekennzeichnet wird. Wie bereits dargestellt, können mit der höchsten Stufe auch prinzipielle Grenzen zur (rechtzeitigen) Entdeckung verbunden sein.

Das „Ablesen" der Risikostufen beziehungsweise Handlungsprioritäten, die hier nur dreistufig (gering/ mittel/hoch) ausgeprägt wurden, ergibt sich durch zeilenweises Matching von Impact/Value über Bedrohungspotenzial (Threat) und Auswahl der passenden Spalte zur „Entdeckung" in der Tabelle. Durch diese Reihenfolge wird auch die Wertigkeit der einzelnen Kriterien hervorgehoben. Die Risikobestimmung beginnt mit der Definition des Schutzbedarfs von Daten, Systemen und Prozessen für eine Organisation oder – wie bei KRITIS – für die Allgemeinheit. Der Impact/Value ist gegen unterschiedlich ausgeprägte Bedrohungen, etwa Viren oder professionell organisierte ATPs, zu schützen. Mit der Einordnung zur Entdeckungswahrscheinlichkeit wird der Aufwand zur Entdeckung der (potenziellen) Bedrohungslage erfasst: So kann dem relativ niedrigen Aufwand zur Entdeckung von Viren beispielsweise die Stufe 2 zugeordnet werden, während der hohe Aufwand für komplexe APTs in die Stufe 4 fällt. Durch die so vollzogene Integration des Entdeckungsaufwands wird dieser bei der Risikoeinstufung und -behandlung hinreichend gewürdigt.

Die zwei Spalten für die Entdeckungswahrscheinlichkeiten zu Stufe 2 und 4 aus Tabelle 1 sind in den beiden Tabellen 2 und 3 noch einmal als zweidimensionale Risikomatrix wiedergegeben. Eine mögliche Interpretation wäre, dass die Nutzung der Risikobewertung mit der Entdeckungswahrscheinlichkeit zwei (2) für die mit grundlegenden Maßnahmen (bspw. des BSI-IT-Grundschutzes) erzielbare Betriebssicherheit und die Matrix im Kontext der Entdeckungswahrscheinlichkeit vier (4) für den KRITIS-Kontext anzuwenden wäre.

		Entdeckung			
Impact/ Value	Threat	1	2	3	4
1	1-3	g	g	g	g
1	4	g	g	g	m
2-3	1	g	g	g	g
4	1	g	g	g	m
2	2	g	m	m	m
2	3	g	m	m	m
2	4	m	m	m	h
3	2	g	m	m	m
3	3	m	m	m	h
3	4	m	m	h	h
4	2	m	m	m	h
4	3	m	m	h	h
4	4	m	h	h	h

Tabelle 1: Ermittlung dreier Risikostufen (gering/mittel/hoch) anhand von qualitativen Werten zu Impact/Value, Bedrohungspotenzial (Threat) sowie Aufwand rechtzeitiger Entdeckung

Impact/ Value	Entdeckung 2			
4	g	m	m	h
3	g	m	m	m
2	g	m	m	m
1	g	g	g	g
	1	2	3	4
	Bedrohungsgrad			

Tabelle 2: Zweidimensionaler Auszug aus Tabelle 1 für die Entdeckungswahrscheinlichkeitsstufe zwei (z. B. für IT-Grundschutz)

Impact/ Value	Entdeckung 4			
4	m	h	h	h
3	g	m	h	h
2	g	m	m	h
1	g	g	g	m
	1	2	3	4
	Bedrohungsgrad			

Tabelle 3: Zweidimensionaler Auszug aus Tabelle 1 für die Entdeckungswahrscheinlichkeitsstufe vier (z. B. für KRITIS-Kontext)

Fazit

Der vorliegende Beitrag beschreibt die Anwendung der FMEA-Methode im Kontext der Informationssicherheit. Durch die Anforderungen für Systeme zur Angriffserkennung (SzA) in KRITIS-Sektoren besteht zu Umsetzungs- und Nachweiszwecken ein Bedarf an nachvollziehbaren Festlegungen – hierbei ist grundlegend auch auf den Aspekt der Erkennungsmöglichkeiten sowie -hindernisse abzuheben. Durch die Anwendung der FMEA-Methodik mit ihrer integrierten Entdeckungswahrscheinlichkeit bietet sich aus Sicht des Autors hierzu ein praktikabler Ansatz.

Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI), Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung, Version 1.0, September 2022, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/ohsza.html

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), Monitoring und Anomalieerkennung in Produktionsnetzwerken, Version 1.0, Februar 2019, www.allianzfuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_134.html

[3] Martin Werdich, FMEA – Einführung und Moderation, Durch systematische Entwicklung zur übersichtlichen Risikominimierung (inkl. Methoden im Umfeld), Vieweg+Teubner, Dezember 2012, ISBN 978-3-8348- 1787-7

[4] ISACA Germany Chapter e. V., Leitfaden Cyber-Sicherheits-Check, Ein Leitfaden zur Durchführung von CyberSicherheits-Checks in der Office-IT von Unternehmen und Behörden, Version 2.0, Februar 2020, www.allianz-fuercybersicherheit.de/Webs/ACS/DE/Informationen-undEmpfehlungen/Informationen-und-weiterfuehrende-Angebote/Cyber-Sicherheitscheck/cyber-sicherheitscheck.html

[5] Martin Werdich, FMEA: Die RPZ ist tot – Es lebe die AP, RiskNET, Mai 2019, www.risknet.de/themen/risknews/die-rpz-ist-tot-es-lebe-die-ap/