#bepartofit

Leitfaden zur Etablierung eines Cyber-Bündnisses

ALLIANZ Industrie 4.0 BADEN-WÜRTTEMBERG

Inhalt

Grußwort 4
Einleitung 6
Management Summary 8
1. Zielsetzung und Rahmenbedingungen 10
2. Phasenmodell für die Cyber-Vorfallsbearbeitung 11
2.1 Präventive Zusammenarbeit 12
2.2 Reaktive Zusammenarbeit 16
2.3 Rollen für die Unterstützung 18
2.4 Unterstützungsfelder eines Cyber-Bündnisses 19
2.4.1 Übergeordnetes Krisenmanagement und Dokumentation 20
2.4.2 Erkennung und Analyse von Cyber-Sicherheitsvorfällen 21
2.4.3 Eindämmung, Beseitigung und Wiederherstellung 21
3. Juristische Aspekte und Rahmenbedingungen 23
3.1 Haftung 23
3.2 Arbeitsrecht 23
3.3 Kartellverbot, Missbrauchs- und Fusionskontrolle 24
3.4 Datenschutz und Informationssicherheit 24
4. Organisation 25
4.1 Struktur und Aufbau eines Cyber-Bündnisses 25
4.2 Kriterien für die Aufnahme in ein Cyber-Bündnis 26
4.3 Budgetausstattung 27
4.4 Incentivierung 27
4.5 Mögliche Cyber-Bündnis-Modelle 28
Übersicht Anhang 30
Projektbeteiligte 31
Impressum 33

Grußwort

Cybersicherheit gewinnt in einer zunehmend digitalisierten und vernetzten Welt immer mehr an Bedeutung. Ein Cyberangriff, der jedes Unternehmen treffen kann, richtet in vielen Fällen massive Schäden an und kann sogar existenzgefährdende Auswirkungen haben. Deshalb muss der Schutz vor Cyberattacken oberste Priorität haben. Und für den Fall, dass ein Unternehmen dennoch Opfer eines Angriffs wird, ist es von zentraler Bedeutung, schnell wieder die volle Handlungsfähigkeit zu erlangen.

Der vorliegende „Leitfaden zur Etablierung eines Cyber-Bündnisses“ kann für Unternehmen hier einen wichtigen Beitrag leisten. Erarbeitet wurde der Leitfaden von einer Projektgruppe, bestehend aus Sicherheitsexperten aus Industrieunternehmen, IT-Unternehmen und Forschungseinrichtungen im Rahmen der Allianz Industrie 4.0 Baden-Württemberg. Diese unternehmerische Eigeninitiative begrüße ich sehr. Der Leitfaden gibt wertvolle Hinweise, wie sich Unternehmen präventiv in Netzwerken zusammenschließen können, deren Mitglieder im Ernstfall füreinander einstehen und für das betroffene Unternehmen ganz konkrete Unterstützungsmaßnahmen organisieren.

Dieses Vorgehen ist ein neuartiger Ansatz, der das Ökosystem Cybersicherheit in Baden-Württemberg um einen weiteren Baustein bereichert. Die Initiative stellt damit eine Ergänzung zu den Angeboten der Sicherheitsbehörden und der

Dr. Nicole Hoffmeister-Kraut
Ministerin für Wirtschaft, Arbeit und Tourismus des Landes Baden-Württemberg
Foto: Katja Bartolec

Unternehmen, die Dienstleistungen auf dem Gebiet der IT-Sicherheit anbieten, dar.

Mein Dank gilt der Allianz Industrie 4.0 Baden-Württemberg, unter deren Federführung der Leitfaden erarbeitet wurde. Die Allianz umfasst rund 50 Partnerorganisationen. Sie unterstützt Industrieunternehmen im Land bei der Digitalisierung und trägt dazu bei, das Land als weltweit führende Region für Industrie 4.0-Technologien zu etablieren. Zusammen mit Informations- und

Unterstützungsangeboten ist vor allem die Vernetzung der beteiligten Branchen und Technologiefelder ein zentrales Handlungsfeld. Kleine und mittlere Unternehmen spielen dabei eine entscheidende Rolle und stehen im Fokus der Allianz Industrie 4.0 Baden-Württemberg, die vom Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg gefördert wird.

Dem Leitfaden wünsche ich eine möglichst große Verbreitung unter den baden-württembergischen Unternehmen. Trotz aller Gefahren, die aus dem Netz drohen können, dürfen wir uns auch in unsicheren Zeiten nicht davon abhalten lassen, die großen Chancen zu ergreifen, die die Digitalisierung eröffnet.

Einleitung

Cybergefahren sind die größte Sorge für Unternehmen weltweit, so das Risk Barometer 2022 der Allianz Global Corporate & Specialty (AGCS). Die Bedrohung durch Ransomwareangriffe, Datenschutzverletzungen oder IT-Ausfälle beunruhigt die Unternehmen sogar noch mehr als Geschäfts- und Lieferkettenunterbrechungen, Naturkatastrophen oder die Covid 19-Pandemie, die alle Unternehmen stark beeinträchtigt haben.

Entspannung ist auch in naher Zukunft nicht zu erwarten. Das Bundesamt für Sicherheit in der Informationstechnik geht in seiner Einschätzung zur Lage der Cybersicherheit in Deutschland von einer Ausweitung der Erpressungsmethoden im Cyber-Raum aus. Insbesondere das sogenannte „Big Game Hunting", also die Erpressung umsatzstarker Unternehmen mit verschlüsselten und exfiltrierten Daten, liege im Trend. Die Bedrohung im Cyber-Raum sei damit so hoch wie nie.
Der Branchenverband BITKOM rechnet in einer Studie vor, dass solche Cyberangriffe und deren Folgen der deutschen Wirtschaft einen jährlichen Schaden von rund 203 Milliarden Euro zufügen. Ein Großteil der Schäden resultiert dabei nicht aus etwaigen Lösegeld- oder Schweigegeldzahlungen, sondern aus den teilweise wochen- oder sogar monatelangen Betriebsunterbrechungen.

Die präventive Stärkung der Cybersicherheit ist deshalb eine Pflichtaufgabe für Wirtschaftsunternehmen. Die derzeitige und zukünftige Bedrohungslage erlaubt es Geschäftsführerinnen und Geschäftsführern jedoch nicht, von einer hundertprozentigen Cybersicherheit ausgehen zu können. Vielmehr ist anzunehmen, dass das eigene Unternehmen trotz adäquater IT-Risikovorsorge selbst Opfer eines schwerwiegenden Cyberangriffs werden wird. Ein schwerwiegender Cyberangriff ist eine Einwirkung auf ein oder mehrere informationstechnische Systeme, die zum Ziel hat, deren Sicherheit ganz oder teilweise zu beeinträchtigen, und dabei zu einer Unterbrechung des Geschäftsbetriebs führt.

Ein gedanklicher Wandel weg vom Prinzip „prevent breach" hin zu „assume breach" ist ein zentraler Baustein für eine zeitgemäße Cybersicherheitsstrategie. Die Folge muss neben dem Blick auf Prävention ein verstärkter Fokus auf Detektion und Reaktion sein. Nur dann können Cyberangriffe entweder rechtzeitig vor einem Großschadensereignis erkannt und unterbunden oder die Betriebsunterbrechung zumindest deutlich verkürzt werden.

Für angegriffene Unternehmen sowie deren Beschäftigte ist der Umgang mit komplexen Cybervorfällen jedoch eine qualitative und quantitative Herausforderung: Zum einen mangelt es den allermeisten Unternehmen an hochspezialisiertem Personal wie Digitale Forensikerinnen und Forensiker oder Incident Responder, aber auch an der zur schnellen Krisenbewältigung notwendigen Anzahl von Personen mit IT-Basiswissen, die beispielsweise Tausende von IT-Geräten in kurzer Zeit neu installieren können. Zum

anderen stellt die Krisenbewältigung für IT-Personal eine Grenzerfahrung dar, da es aus dem bestenfalls seit Jahren andauernden Normalbetrieb nicht mit den komplexen Anforderungen einer Krisensituation vertraut ist.
Selbstredend versucht insbesondere der IT-Dienstleistermarkt diese reaktiven Bedarfe von Wirtschaftsunternehmen bestmöglich zu decken. In der Vergangenheit zeigte sich allerdings, dass auch Dienstleisterkapazitäten beschränkt sind und vor allem bei einer Vielzahl gleichzeitiger Cyberangriffe – z. B. über die IT-Lieferkette – nicht allen Hilfe suchenden Unternehmen ausreichend Unterstützung angeboten werden kann.

Auch die reaktiven Hilfsangebote der Cybersicherheits- und Strafverfolgungsbehörden können diese Kapazitätslücke für den Großteil der Wirtschaftsunternehmen nicht schließen. Entweder kommt die staatliche Unterstützung nur der eingeschränkten Zielgruppe Kritischer Infrastrukturen (KRITIS) zugute oder sie beschränkt sich aus rechtlichen Gründen auf die Aspekte der Strafverfolgung innerhalb der ersten Vorfallsbehandlung. Sie umfasst jedoch nicht die vollständige Wiederherstellung des Geschäftsbetriebs.

Wie können Unternehmen also überhaupt eine IT-Krise bewältigen? Ein entscheidendes Element des Krisenmanagements kann die gegenseitige Unterstützung von Unternehmen für Unternehmen in „Cyber-Bündnissen“ nach schwerwiegenden Cyberangriffen in den Phasen Detektion und Reaktion inklusive Wiederherstellung sein.
Eine informelle wechselseitige Unterstützung von Industrieunternehmen während eines Cyberangriffs im Jahr 2021 im Raum Esslingen hatte solche Nutzeneffekte praktisch belegt. Im Rahmen der Nachbetrachtung zeigte sich jedoch, dass die Beantwortung grundlegender rechtlicher und organisatorischer Fragestellungen die Grundlage für die Verstetigung und Ausweitung der gegenseitigen Unterstützung darstellt.
Der vorliegende Leitfaden unterstützt Vorbereitung, Planung und Aufbau von Cyber-Bündnissen in der Wirtschaft durch Best Practices und die Klärung rechtlicher Fragestellungen. Gleichzeitig wird ein Rahmen für eine verstetigte und rechtskonforme gegenseitige Unterstützung zwischen Wirtschaftsunternehmen im Cyber-Krisenfall geboten.

Dieser Leitfaden wird von der Allianz Industrie 4.0 Baden-Württemberg, deren Koordinierungsstelle beim VDMA e. V. Baden-Württemberg angesiedelt ist, herausgegeben. Die Allianz Industrie 4.0 Baden-Württemberg wird vom Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg gefördert. Die an der inhaltlichen Erarbeitung des Leitfadens Beteiligten sind unter „Projektbeteiligte“ aufgeführt.

Der Aufbau eines Cyber-Bündnisses und die Mitgliedschaft in einem solchen steht allen Unternehmen – explizit auch solchen ohne Mitgliedschaft beim VDMA – offen.

Management Summary

Die Bedrohung für Unternehmen, Opfer eines schwerwiegenden Cyberangriffs zu werden, ist laut Einschätzung von Behörden und der IT-Sicherheitsindustrie so hoch wie nie. Unternehmerische Vorbereitungen für die Erkennung und die Reaktion auf solche IT-Sicherheitsvorfälle sind deshalb unabdingbar.
Das dafür notwendige Personal ist in den betroffenen Unternehmen jedoch meist nicht in ausreichender Anzahl und mit der notwendigen Qualifikation vorhanden. Aus Kapazitäts- und rechtlichen Gründen können auch IT-Sicherheitsdienstleister und Behörden diese Lücke nicht vollständig schließen.

Die gegenseitige Unterstützung von Unternehmen für Unternehmen in „Cyber-Bündnissen" nach schwerwiegenden Cyberangriffen in den Incident Response-Phasen Detektion, Reaktion und Wiederherstellung kann folglich ein wichtiger Baustein im unternehmerischen Krisenmanagement sein.
Gleichzeitig trägt die Mitgliedschaft in einem Cyber-Bündnis einerseits den Compliance-Anforderungen an die Geschäftsführung nach einem umfassenden Risikomanagement Rechnung und kann sich vorteilhaft auf die Konditionen einer Cyber-Versicherung auswirken.

Die Gründung und der Betrieb eines Cyber-Bündnisses setzen jedoch die Klärung rechtlicher und organisatorischer Fragestellungen voraus. Dieser Leitfaden unterstützt die Vorbereitung, die Planung, den Aufbau sowie den Betrieb von Cyber-Bündnissen in der Wirtschaft und richtet sich an Unternehmen aller Größen und Branchen.

Mit Blick auf die Organisation von Cyber-Bündnissen sprechen sich die Verfasserinnen und Verfasser für eine dezentrale organisatorische Gliederung von (mehreren unterschiedlichen) Cyber-Bündnissen im Sinne einer Wabenstruktur aus. Dezentrale Cyber-Bündnisse stellen jeweils eine funktionsfähige und in sich geschlossene Einheit im Sinne einer Netzwerkwabe dar, die sich im Bedarfsfall gegenseitig unterstützen können.
Relevante Kriterien für die Aufnahme in ein Cyber-Bündnis können zum Beispiel die regionale Nähe der Mitgliedsunternehmen, deren Branchenzugehörigkeit, Unternehmensgröße oder Homogenität der IT-Infrastruktur sein.

Die durch juristische Experten in diesem Leitfaden getroffene haftungsrechtliche, kartell- und wettbewerbsrechtliche sowie arbeitsrechtliche Einschätzung macht deutlich, dass Cyber-Bündnisse rechtskonform etabliert und betrieben werden können.

Aus juristischer Sicht sind verschiedene Organisationsformen für Cyber-Bündnisse möglich. Die Modelle „Handschlag", „Handschlag Plus" und „verbindliche Organisation" unterscheiden sich in ihrer Rechtsform. Mit den unterschiedlichen

Organisationsformen gehen deutliche Unterschiede in der Verbindlichkeit und damit auch in der Verlässlichkeit der Hilfeleistung im Krisenfall einher, die jedoch dem jeweiligen Aufwand zur Steuerung des Cyber-Bündnisses diametral gegenüberstehen.

Ist ein Cyber-Bündnis etabliert, empfiehlt sich eine regelmäßige Zusammenarbeit schon in „Friedenszeiten", um die Strukturen (bspw. durch das Vorhalten von Ressourcen) und Prozesse (bspw. durch Übungen oder regelmäßigen Austausch und Abstimmungen der Bündnismitglieder) zu schärfen. Denkbar ist auch eine Verpflichtung der Bündnismitglieder zur Bereitstellung eines Budgets mit dem Ziel der gemeinsamen Beschaffung von IT-Hardware durch die Bündnismitglieder oder eine mögliche Kompensation für Hilfe leistende Unternehmen.

Nach Eintritt des Bündnisfalles durch einen schwerwiegenden Cyberangriff auf ein Bündnismitglied sind – abhängig vom konkreten Schadensereignis, dem Bedarf des Hilfe suchenden Unternehmens und den Kompetenzen der helfenden Bündnismitglieder – unterschiedliche reaktive Unterstützungsleistungen denkbar. Grundsätzlich gliedern sich die Unterstützungsleistungen in operative und beratende personelle sowie materielle Unterstützung. Die häufigsten Unterstützungsfelder sind das übergeordnete Krisenmanagement, die Erkennung und Analyse von Cyber-Sicherheitsvorfällen sowie die Eindämmung und Beseitigung des durch den Cyberangriff entstandenen Schadens und die Wiederherstellung des Normalzustandes.

1. Zielsetzung und Rahmenbedingungen

Für angegriffene Unternehmen sowie deren Beschäftigte ist die Bewältigung von schwerwiegenden Cyberangriffen eine qualitative und quantitative Herausforderung. Das in den betroffenen Unternehmen beschäftigte IT-Personal reicht oftmals zur schnellen Rückkehr in den Normalbetrieb nicht aus oder ist auf die Extremsituation einer Krise nicht ausreichend vorbereitet bzw. dafür nicht qualifiziert. Zudem können weder der IT-Dienstleistermarkt noch staatliche Stellen diese Kapazitätslücke vollständig schließen.

Der gegenseitigen Unterstützung von Unternehmen in „Cyber-Bündnissen" nach schwerwiegenden Cyberangriffen in den Phasen Detektion und Reaktion inklusive Wiederherstellung kann deshalb entscheidende Bedeutung im unternehmerischen Krisenmanagement zukommen. Solche Cyber-Bündnisse sind komplementär und nicht konkurrierend zu den Leistungen von Behörden und privaten IT-Dienstleistern zu sehen.

Cyber-Bündnisse bieten angegriffenen, Hilfe suchenden Unternehmen Unterstützung durch pragmatische Schadensidentifizierung, -eindämmung und -beseitigung sowie Wiederherstellung. Diese Hilfe kann kostenlos oder zumindest kostengünstig angeboten werden. Etablierte Beziehungen und gegenseitiges Vertrauen zwischen den Bündnismitgliedern erhöhen die Qualität der Krisenreaktion, die zudem zielgerichtet auf (IT-)Bedürfnisse von (produzierenden) Unternehmen ausgerichtet ist und, auch kurzfristig, hohe personelle „Schlagkraft" entwickeln kann. Für die helfenden Unternehmen stellt die Krisenbewältigung wiederum eine wertvolle und oftmals einzigartige Lernerfahrung für die Vorbereitung auf den eigenen potenziellen Krisenfall dar.

Die Gründung und der Betrieb eines Cyber-Bündnisses setzen jedoch die Klärung rechtlicher und organisatorischer Themen voraus. Einerseits stellt allein die Organisation eines Netzwerks über Unternehmensgrenzen hin-weg die Beteiligten vor besondere Herausforderungen. Die Vor- und Nachteile möglicher Organisationsformen eines Cyber-Bündnisses müssen individuell abgewogen werden. Andererseits müssen die Strukturen des Netzwerks kompatibel mit den jeweiligen Strukturen und Kulturen der einzelnen Mitglieder sein. Außerdem ist fraglich, welche zusätzlichen Risiken für das einzelne Mitglied entstehen, indem es externe Unterstützende in seinen Krisenmanagement-Prozess integriert. Das Vertrauen in die Integrität, aber auch in die Leistungsfähigkeit der Netzwerkpartner mag hier entscheidend sein.

Daneben kann die Regelung haftungsrechtlicher, kartell- und wettbewerbsrechtlicher sowie arbeitsrechtlicher Themen eine notwendige Vorbedingung eines Beitrittskandidaten für den Eintritt in ein Cyber-Bündnis darstellen. Schließlich sind auch kommerzielle Aspekte zu berücksichtigen: von der möglichen gemeinsamen Beschaffung von IT-Hardware durch die Bündnismitglieder über die kontinuierlichen Managementaufwände zur Bündnispflege bis hin zur möglichen Kompensation für Hilfe leistende Unternehmen.

Um nach Gründung eines Cyber-Bündnisses fortlaufend Stabilität und Leistungsfähigkeit zu gewährleisten, berücksichtigen Cyber-Bündnisse bestenfalls die praktischen Rahmenbedingungen (z. B. gleiche IT-Hardwarehersteller), die örtliche Distanz (z. B. bzgl. Reaktionszeiten), die fachlichen Bedürfnisse (z. B. besondere Risikoexposition) und rechtliche Spielräume (z. B. vorhandene innerbetriebliche Regelungen) der Bündnismitglieder. Daher erscheint die Gründung mehrerer Cyber-Bündnisse im Sinne einer Wabenstruktur anstelle eines einzigen großflächigen Cyber-Bündnisses sinnvoll.

Dieser Leitfaden richtet sich deshalb grundsätzlich an Unternehmen aller Größen und Branchen. Erstmalig wird in Deutschland so konkret wie nötig, aber so generisch wie möglich die Idee von Cyber-Bündnissen skizziert sowie Vorbereitung, Planung, Aufbau und Betrieb von Cyber-Bündnissen in der Wirtschaft beschrieben. Die Autorinnen und Autoren erhoffen sich dadurch einen Skaleneffekt, bei dem die verschiedenen Cyber-Bündnisse in ihrer Gesamtheit die Resilienz der Wirtschaft gegen Cyberangriffe stärken.

Der Leitfaden soll mit Best Practices von erfahrenen IT-Sicherheitsverantwortlichen bei den praktischen Herausforderungen helfen. Rechtliche Fragen werden im Kapitel „Juristische Aspekte" durch eine Fachanwaltskanzlei beantwortet. Als praktische Hilfe finden sich im Anhang notwendige Mustervereinbarungen und -verträge, mit denen bereits im Vorfeld Rechtssicherheit zwischen den Bündnismitgliedern geschaffen werden kann.

Gleichzeitig erhebt der Leitfaden keinen Anspruch auf Vollständigkeit. Er kann und muss entsprechend der individuellen Bedürfnisse einzelner Cyber-Bündnisse und ihrer Mitglieder angepasst bzw. erweitert, vor allem aber auf Grundlage zu gewinnender Erfahrungswerte aus ersten praktischen Cyber-Bündnissen kontinuierlich verbessert werden.

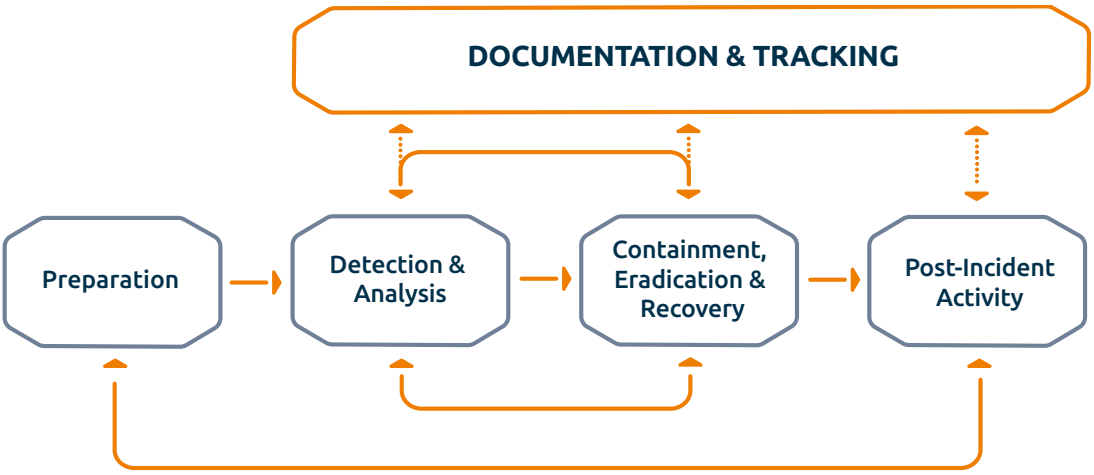
2. Phasenmodell für die Cyber-Vorfallsbearbeitung

Den Kern der in diesem Leitfaden beleuchteten Cyber-Bündnisse bildet die gegenseitige Unterstützung von Unternehmen für Unternehmen während der Erkennung eines schwerwiegenden Cyberangriffs, insbesondere bei der Reaktion auf einen solchen und der notwendigen Wiederherstellung des Normalzustandes.

Als Leitbild für eine gelingende Bewältigung eines Cyberangriffs kann sowohl in einzelnen Unternehmen als auch in einem Cyber-Bündnis der im „Computer Security Incident Handling Guide" des US-amerikanischen National Institute of Standards and Technology (NIST) als de facto Industriestandard beschriebene „Incident Response Life Cycle " herangezogen werden.

Der „Incident Response Life Cycle “ strukturiert die Vorfallsreaktion in die Phasen

- Vorbereitung,
- Erkennung und Analyse,
- Eindämmung, Beseitigung und Wiederherstellung sowie
- nachgelagerte Aktivitäten, insbesondere Nachbereitung und kontinuierliche Verbesserung.



Grafikquelle: in Anlehnung an Computer Security Incident Handling Guide (nist.gov), S. 21

2.1 Präventive Zusammenarbeit

Im Kontext von Cyber-Bündnissen sind vorbereitende Maßnahmen von jedem Bündnismitglied selbst umzusetzen. Nicht zuletzt im eigenen Interesse, um auch Cyber-Sicherheitsvorfälle unterhalb der „Krisenschwelle“ und ohne Unterstützung aus dem Cyber-Bündnis selbst erfolgreich zu bearbeiten.

Die Phase der Vorbereitung umfasst den Aufbau sowie die Aus- und kontinuierliche Weiterbildung eines Incident Response-Teams. Daneben ist es in dieser Phase angezeigt, die notwendigen Werkzeuge und Ressourcen zu beschaffen, um adäquat auf auftretende Sicherheitsvorfälle reagieren zu können. Hohe Priorität hat außerdem die Definition der Prozessschritte zur Vorfallsbearbeitung und deren Dokumentation in Form von Reaktionsplänen auf verschiedene Cyberangriffsformen. Zu klären sind in dieser Phase auch die Schnittstellen zu allen an der Incident Response beteiligten Stellen innerhalb des Unternehmens.

Diese präventiven Vorbereitungen zur Bewältigung eines Bündnisfalls in Form eines schwerwiegenden Cyberangriffs auf Mitgliedsunternehmen sind aber ebenso auf Ebene der Cyber-Bündnisse relevant, wenngleich diese regelmäßig nicht denselben Umfang und die Detailtiefe wie auf individueller Unternehmensebene aufweisen dürften.

Aufbauend auf den Strukturen, die im Kapitel „Organisation" vorgeschlagen werden, empfiehlt es sich, schon in „Friedenszeiten" eine regelmäßige Zusammenarbeit anzustreben, um die Strukturen zu verstetigen.

Grundlage der Zusammenarbeit ist Vertrauen. Um Risiken gemeinsam begegnen zu können, ist daher die Vertrauensbildung durch enge Zusammenarbeit, Offenheit und regelmäßige Kommunikation anzustreben. Absolute Integrität und Aufrichtigkeit der handelnden Personen sowie die Absicht, sich dauerhaft und aktiv einzubringen, sind Voraussetzung für eine erfolgreiche Umsetzung.

Fokus dieses Leitfadens ist es, die unternehmensübergreifende Zusammenarbeit zu skizzieren.

Diese Zusammenarbeit und die Unterstützung daraus befreit das einzelne Unternehmen keinesfalls davon, selbst geeignete Maßnahmen im Rahmen eines Cyber Security Management Systems (CSMS) zu treffen. Mindestanforderungen, die für jedes Unternehmen gelten, um eine faire Zusammenarbeit auf Augenhöhe zu gewährleisten, umfassen das gesamte Spektrum von technischen Vorbereitungsmaßnahmen über die Qualifikation der Helferinnen und Helfer bis hin zu organisatorischen Maßnahmen in allen betroffenen Unternehmen. Es ist ratsam, sich an gängigen Standards zu orientieren (BSI-Grundschutz, ISO27001 etc.). Wichtig dabei ist, dass sowohl die Leistungsfähigkeiten der einzelnen Netzwerkmitglieder als auch die Risiken angemessen verteilt sind.

Idealerweise unterstützen sich Netzwerkmitglieder, die ähnliche Unternehmensstandards einsetzen, da in diesem Fall nur geringe Einarbeitungsaufwände entstehen. Präventiv sollten sich daher die Mitglieder hinsichtlich ihrer Standards austauschen, um für den Notfall bevorzugte Partner zu finden.

Die Formate der Zusammenarbeit können sein:

- **Austauschformate** zu aktuellen Bedrohungen und Schwachstellen in Systemen und Best Practices beim Umgang mit diesen.
- **Gemeinsame Übungen** der an der Krisenorganisation beteiligten Mitarbeiterinnen und Mitarbeiter. Diese Übungen dienen einerseits dem Training der beteiligten Personen, andererseits der Entwicklung und Verbesserung von Notfallprozessen.
- **Schulungen** zu spezialisierten Themen können gemeinsam organisiert werden. Durch eine größere Teilnehmendenzahl aus dem Pool der beteiligten Unternehmen lassen sich Synergien schaffen. Bei der Einbindung von Dienstleistern sind Aspekte des Kartellrechts zu beachten.

Mit Blick auf die konkrete Anforderung und Gewährung von Unterstützung in einem Cyber-Bündnis sind darüber hinaus bereits präventiv konkrete Rahmenbedingungen festzulegen.

Ein wesentliches Ziel eines Cyber-Bündnisses ist die schnelle und zielgerichtete Unterstützung bei einem Cyberangriff. Für eine schnelle Reaktion ist zu empfehlen, Alarmpläne auszuarbeiten, in denen Verantwortlichkeiten und Kommunikationswege festgelegt werden.

Die definierten Unterstützungsangebote des Cyber-Bündnisses müssen im Bedarfsfall unkompliziert und unbürokratisch abgerufen werden können. Hierfür sollten im Vorfeld zwischen den Bündnismitgliedern verbindliche Definitionen und Prozesse erarbeitet werden.

Phasenmodell/Alarmierungsprozess

Definition Bündnisfall

Die wichtigste Definition im vorliegenden Kontext ist die klare Beschreibung der Gegebenheiten, die vorliegen müssen, um einen Bündnisfall auszurufen, der zur Anforderung von Unterstützungsleistungen aus dem Cyber-Bündnis berechtigt. Um die individuellen Ausgestaltungsmöglichkeiten nicht zu schmälern, kann an dieser Stelle keine allgemeingültige Definition vermerkt werden. Die nachfolgenden Ausführungen dienen lediglich zur Herstellung eines einheitlichen Verständnisses und zur groben Orientierung:

1. Die Parteien vereinbaren, dass sie sich im Falle eines schwerwiegenden Cyberangriffs auf eine oder mehrere Parteien gegenseitig im definierten Umfang unterstützen.
2. Bei einem schwerwiegenden Cyberangriff handelt es sich um eine Einwirkung auf ein oder mehrere informationstechnische Systeme, die zum Ziel hat, deren Sicherheit ganz oder teilweise zu beeinträchtigen und dabei zu einer Unterbrechung des Geschäftsschäftsbetriebs führt.

Alarmierungsprozess

Sobald ein Bündnisfall eingetreten ist und die betroffene Partei Unterstützung aus dem Cyber-Bündnis in Anspruch nehmen möchte, ist das Bündnis über einen vorab festgelegten Prozess zu alarmieren. Ziel sollte es sein, eine kurze Besprechung zu ermöglichen, in der die angegriffene Partei den anderen Bündnismitgliedern einen kurzen Lageüberblick gibt und die konkreten Unterstützungsbedarfe skizziert.

Folgende Aspekte sollten hierbei berücksichtigt werden:

LEITFRAGEN	BEISPIELE
Über welchen Kanal werden die Bündnismitglieder im Bündnisfall alarmiert?	Messenger-Gruppe, Alarmierungstool, E-Mail, Telefonkette etc.
Welche Personen werden alarmiert?	CIO, CISO etc.
Wie findet die angestrebte Besprechung statt?	virtuelle ad hoc-Besprechung, Telefonkonferenz, persönliches Meeting etc.
Wie viel Zeit darf zwischen Alarmierung und der Durchführung der angestrebten Besprechung liegen?	unverzüglich, sechs Stunden, 24 Stunden etc.

Anforderungsprozess

Da schwerwiegende Cyberangriffe in der Regel eine hohe Dynamik und skalierende Schäden mit sich bringen, sollte die Unterstützungsanforderung wenig formalisiert sein und ein hohes Maß an Flexibilität aufweisen.

Bei der Besprechung zu einem abgestimmten Termin in einem angemessenen Zeitraum nach der Alarmierung sollte eine bevollmächtigte Person aus jeder Partei des Cyber-Bündnisses anwesend sein. Der Ablauf der Besprechung gestaltet sich wie folgt:

a. Begrüßung durch die betroffene Partei.
b. Kurze Information zur Lage inkl. Bewertung der Situation durch die betroffene Partei.
c. Genaue Darstellung der Unterstützungsbedarfe durch die betroffene Partei auf Basis der vorab festgelegten Unterstützungsmöglichkeiten des Cyber-Bündnisses.
d. Möglichkeit für Rückfragen.
e. Vereinbarung, bis zu welchem Zeitpunkt Rückmeldungen zur Anforderung seitens aller Bündnismitglieder bei der betroffenen Partei eingehen müssen.

Nach der Besprechung prüfen alle Bündnismitglieder, ob und ggf. in welchem Umfang sie die angegriffene Partei auf Basis deren Bedarfslage unterstützen können und geben dieser eine verbindliche Rückmeldung.

Auf Basis der eingegangenen Rückmeldungen nimmt die betroffene Partei Kontakt mit den unterstützenden Bündnismitgliedern auf und stimmt die weiteren Schritte ab.

2.2 Reaktive Zusammenarbeit

In den reaktiven Phasen des „Incident Response Life Cycle" liegt der Fokus zunächst auf der Erkennung und der Analyse von Cyber-Sicherheitsvorfällen. Die Erkennung von Cyber-Sicherheitsvorfällen kann sich auf verschiedene Informationsquellen stützen. In der Praxis sind dies insbesondere Log-Daten aus IT-Systemen – idealerweise manipulationssicher gespeichert, korreliert und automatisiert überwacht –, Meldungen von Beschäftigten des Unternehmens oder Meldungen von externen Dritten, z. B. Behörden.
Nach der Erkennung ist ein Cyber-Sicherheitsvorfall anhand von Kriterien zu kategorisieren und mit Blick auf die weitere Bearbeitung zu priorisieren. Alle relevanten mit dem Vorfall in Bezug stehenden Informationen und Handlungen sind in einem Vorfallsmanagementsystem zu dokumentieren.
In der Regel sind in dieser Phase tiefer gehende, teilweise digital-forensische Untersuchungen erforderlich, um das potenzielle Schadensausmaß abzuschätzen. Auf Grundlage des zu erwartenden oder bereits eingetretenen Schadensbildes ist bereits zu diesem Zeitpunkt eine Eskalation an höhere Hierarchieebenen oder sogar die Unternehmensleitung notwendig, um ausreichend qualifizierte Personalressourcen für die weiteren Phasen heranzuziehen.
Die zeitlich und inhaltlich umfangreichste Phase stellt insbesondere bei schwerwiegenden Cyberangriffen die Phase der Eindämmung des schadhaften Ereignisses, die Beseitigung der Schadensursache und die Wiederherstellung des Normalzustandes dar. Zunächst ist durch die Incident Responder eine Strategie zur Eindämmung des (potenziellen) Schadens festzulegen. Vordefinierte Eindämmungsstrategien für unterschiedliche Fallkonstellationen beschleunigen diesen Prozess, da die Vor- und Nachteile der Varianten abgewogen und die Entscheidungsalternativen bestenfalls durch die Unternehmensleitung genehmigt sind. Beispielhaft ist aus der Praxis die Trennung des gesamten internen Netzwerks vom Internet mit der Folge des großflächigen Ausfalls unternehmenskritischer Prozesse zu nennen.

Als Zwischenschritt nach der Eindämmung des Schadensereignisses und vor der Beseitigung der Ursache sind auch digital-forensische Maßnahmen zur genauen Identifizierung der Ursache und zur Sammlung gerichtsverwertbarer Nachweise zu erwägen. Diese bilden die unverzichtbare Grundlage für etwaige arbeitsrechtliche, strafrechtliche oder versicherungsrechtliche Folgemaßnahmen. Gerade diese im Unternehmensalltag äußerst selten praktizierte digital-forensische Spurensicherung ist in der ersten Phase des „Incident Response Life Cycle" prozessual und durch Ausbildung qualifizierter

Mitarbeiterinnen und Mitarbeiter umfassend vorzubereiten, wenn sie im Zuge der dynamischen Vorfallsbearbeitung mit adäquatem Qualitätsstandard ausgeführt werden soll.

Die Beseitigung der Schadensursache geht oftmals unmittelbar mit der Wiederherstellung des Zustandes vor dem Schadensereignis einher. Möglichst schon im Vorfeld sind hierbei mit dem Ziel der Beschleunigung geeignete Bereinigungs- und Wiederherstellungsstrategien zu entwerfen und – soweit vor einem konkreten Schadensereignis möglich – auf Basis einer Folgeabschätzung mit der Unternehmensleitung zu vereinbaren. Als praxisrelevantes Beispiel dient die Frage, ob nach einem schwerwiegenden Cyberangriff nur nachweislich infizierte Notebooks/PCs zur Beseitigung von Schadsoftwareinfektionen neu installiert werden sollten oder ob eine Neuinstallation für sämtliche, potenziell als infiziert geltende Notebooks/PCs angezeigt ist, was den großflächigen Ausfall unternehmenskritischer Prozesse zur Folge haben dürfte.

Im Anschluss an die akute Phase der Vorfallsreaktion wird eine Nachbereitung der Aktivitäten – auf Unternehmensebene mit den beteiligten Personen(gruppen), auf Ebene des Cyber-Bündnisses mit den helfenden Unternehmen – empfohlen. Diese bildet den Ausgangspunkt für einen Prozess zur kontinuierlichen Verbesserung, in dem zum einen Maßnahmen zur zukünftigen Verhütung desselben oder ähnlicher Schadensereignisse identifiziert, zum anderen Maßnahmen zur Steigerung von Effektivität und Effizienz des Incident Response-Prozesses abgeleitet werden.

Idealerweise sind die dargestellten Phasen einerseits durch eine übergeordnete Steuerungsebene der Vorfallsbearbeitung eingerahmt, die die technischen Aspekte der Incident Response mit den nicht-technischen Anforderungen der Unternehmensleitung verknüpft. Andererseits sollte eine zuständige Stelle die durchgeführten Maßnahmen kontinuierlich dokumentieren.

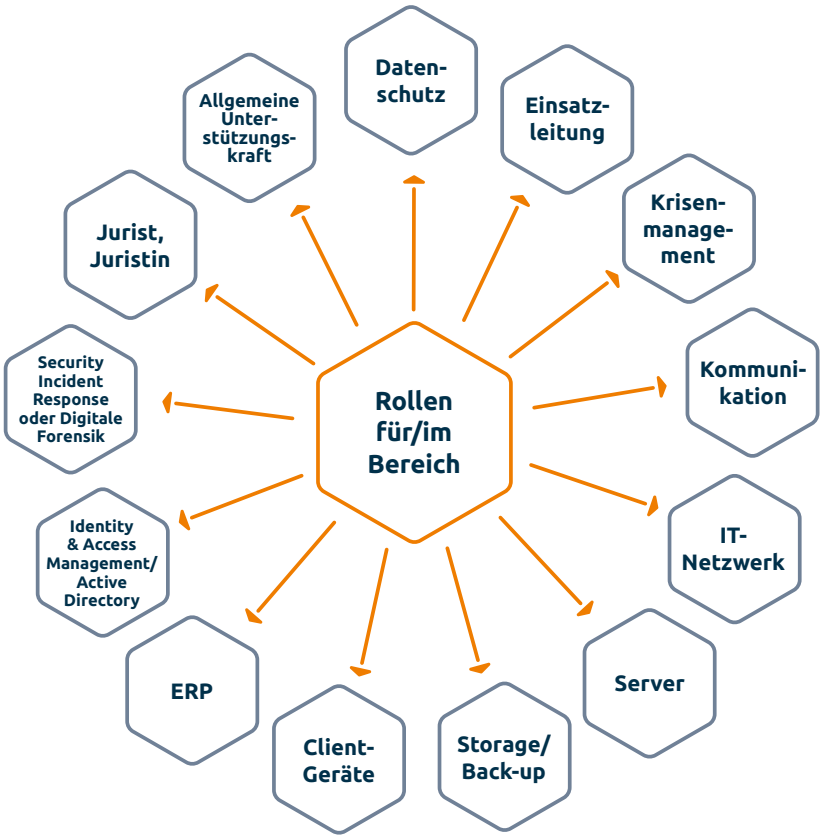
Gerade bei einer Beteiligung mehrerer Bündnismitglieder ist ein stringentes Krisenmanagement notwendig, das den Überblick über die Sachlage behält und die erforderlichen nächsten Schritte durch die an der Vorfallsbearbeitung internen und externen (insb. Bündnismitglieder) Schritte koordiniert.

Eine fortlaufende, konsistente Dokumentation der Incident Response-Tätigkeiten ist die Grundlage für das erfolgreiche Krisenmanagement. Ohne entsprechende Aufzeichnungen in der Rückschau kann es sonst sehr schwierig sein, den Verlauf der Incident Response zu rekonstruieren.
Eine vollständige Dokumentation ist daher eine entscheidende Grundlage für die dargestellte Nachbereitung und den kontinuierlichen Verbesserungsprozess – für das angegriffene Unternehmen selbst, aber auch als Lernerfahrung für die helfenden Bündnismitglieder. Darüber hinaus sind detaillierte schriftliche Aufzeichnungen über die Vorfallsbearbeitung für eine etwaige Geltendmachung von Ansprüchen aus möglicherweise beim Hilfe suchenden Unternehmen vorhandenen Cyber-Versicherungen relevant.

2.3 Rollen für die Unterstützung

Vorab definierte Rollen können im Falle eines Cyberangriffs Zeit sparen und damit der schnellen Eindämmung von Gefahren dienen. Die definierten Rollen erleichtern Fragestellungen in Bezug auf nötige Zugänge und das fachliche Gebiet der Unterstützung. Dies erleichtert das Ressourcenmanagement für Bündnismitglieder und das betroffene Unternehmen. Darüber hinaus können über die Rollen vorab Verantwortlichkeiten grob skizziert werden. Die Autorinnen und Autoren empfehlen, gemäß folgendem Beispiel eine Liste von Rollen innerhalb eines Bündnisses zu definieren und zu pflegen.

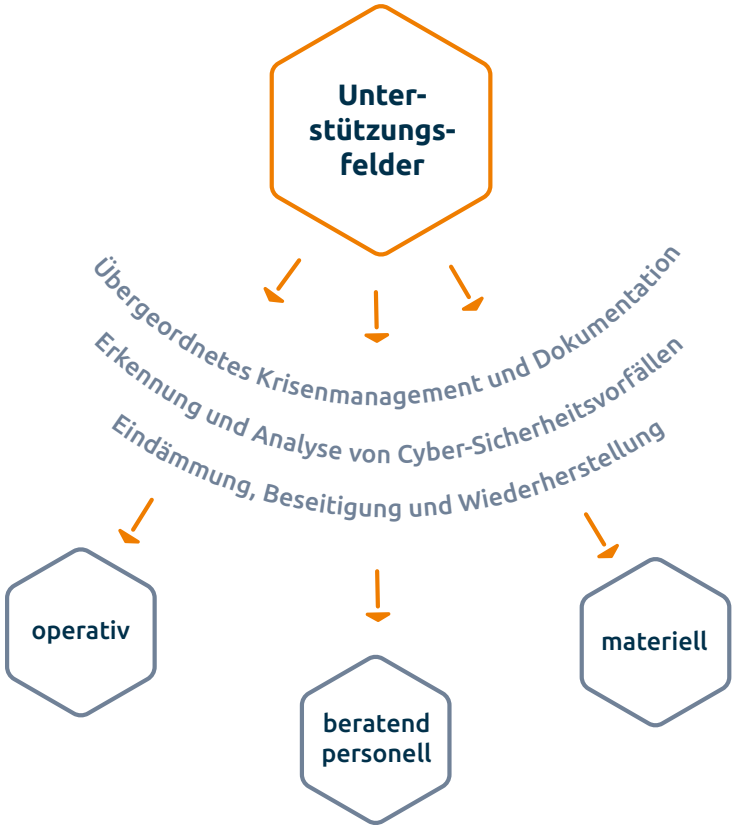
Exemplarische Rollen:



2.4 Unterstützungsfelder eines Cyber-Bündnisses

Die denkbaren Unterstützungsleistungen von Mitgliedern eines Cyber-Bündnisses sind mannigfaltig und letztlich abhängig vom konkreten Schadensereignis, dem Bedarf des Hilfe suchenden Unternehmens und den Kompetenzen der helfenden Bündnismitglieder.

Grundsätzlich gliedern sich die Unterstützungsleistungen in operative, beratende personelle und materielle Unterstützung. Im Folgenden werden Unterstützungsleistungen in Cyber-Bündnissen dargestellt, die von IT-Sicherheitsverantwortlichen als geeignet und praktikabel für die gemeinsame Bewältigung eines schwerwiegenden Cyberangriffes eingeschätzt werden.



2.4.1 Übergeordnetes Krisenmanagement und Dokumentation

Helfende Bündnismitglieder können erfahrene Krisenmanagerinnen und Krisenmanager zur Unterstützung der im Hilfe suchenden Unternehmen benannten Leitung der Krisenmanagementorganisation entsenden. Zunächst erscheint es dabei risikoreich, die Steuerung des Krisenmanagements gesamthaft einem helfenden Bündnismitglied zu übertragen.

Praxisnäher könnte die anlassbezogene Unterstützung der Krisenmanagerin/des Krisenmanagers bei der Umsetzung von organisatorischen und administrativen Tätigkeiten oder die eigenverantwortliche Leitung von Teilbereichen des Krisenmanagements sein. Beispielsweise für die Koordination fachbezogener Aufgaben in der Krisenmanagementorganisation des Hilfe suchenden Mitglieds. Dafür wären erfahrene Projektmanagerinnen und Projektmanager (auch ohne Cybersicherheitswissen) aus helfenden Unternehmen geeignet.

Weitaus technischer kann eine Unterstützung durch Bündnismitglieder in Form der Koordination der technischen Vorfallsanalyse unter Einbezug aller beteiligter IT-Teams (z. B. Client Management-Team, Server Management-Team, Netzwerk Management-Team) sein.

Weitere personelle Unterstützung in den das Krisenmanagement und die technische Vorfallsbearbeitung begleitenden Disziplinen kann durch Versicherungsexpertinnen und -experten, Juristinnen und Juristen, Datenschützerinnen und Datenschützer sowie IT-Einkäuferinnen und -Einkäufer erfolgen. Die Bereitstellung einer Cyber-Versicherungsexpertin/eines Cyber-Versicherungsexperten ist zur Unterstützung der Rechts- bzw. Versicherungsabteilung des Hilfe suchenden Unternehmens bei der Meldung und Abwicklung des Schadensfalls sowie bei der Kommunikation mit der Versicherung denkbar.

Dabei helfen die Bündnismitglieder beratend oder unmittelbar bei

- der Meldung und Abwicklung des Schadensfalls sowie bei der Kommunikation mit der Cyber-Versicherung,
- der Beschaffung von IT-Hardware und -Lizenzen für das Hilfe suchende Unternehmen,
- der Beurteilung und dem Vollzug der Meldepflichten (z. B. Datenschutz, Störfall, KRITIS etc.),
- notwendigen datenschutzrechtlichen Prüfungen,
- möglichen Lösegeldforderungen (rechtlich problematisch, siehe Anlage 1, Abschnitt B, 1.3.2.2).

Weiterhin ist die Unterstützung durch (kurzfristig auch eine hohe Anzahl von) Personen aus helfenden Unternehmen ohne IT-Fachkompetenzen zur Organisation von Verpflegung, Geländekontrolle, Logistik oder Personalplanung denkbar. Gleiches gilt für die Unterstützung der Dokumentation des Krisenmanagements.

2.4.2 Erkennung und Analyse von Cyber-Sicherheitsvorfällen

Nicht selten werden in der Praxis aufgrund der Vielzahl von Verdachtsmeldungen aus dem Security-Monitoring klare Anzeichen auf einen ernst zu nehmenden Cyber-Sicherheitsvorfall übersehen oder falsch interpretiert. Dadurch kann es zur Verzögerung der zeitkritischen Incident Response oder zum gänzlichen Verzicht auf Response-Maßnahmen kommen.

Bündnismitglieder können in dieser frühen Phase vor allem mit qualifizierten Personen aus den Bereichen des Security Information und Event Managements bzw. der Security Operations dabei helfen, erste Verdachtsindikatoren eines möglicherweise schwerwiegenden Cyberangriffs zu sichten und im Rahmen einer gemeinsamen Analyse als „Sparringspartner“ zu bewerten.

2.4.3 Eindämmung, Beseitigung und Wiederherstellung

Im Zuge der Eindämmung und Datensicherung können Personen mit digital-forensischen Kompetenzen aus helfenden Unternehmen entweder unmittelbar selbst forensische Sicherungen erstellen und Untersuchungen vornehmen oder die vom angegriffenen Unternehmen beauftragten IT-Dienstleister bzw. um Hilfe ersuchten Behörden unterstützen.

Die anschließende Beseitigung der Schadensursache und die Wiederherstellung des Normalzustandes ist aus Sicht der (teilweise schon selbst betroffenen) IT-Sicherheitsverantwortlichen das Haupteinsatzgebiet der Bündnismitglieder.
Das wahrscheinlichste Szenario für einen Cyber-Bündnisfall ist ein schwerwiegender Cyberangriff mit Einwirkung auf die IT-Infrastruktur und damit die Geschäftsprozesse des angegriffenen Unternehmens. In solchen Fällen ist regelmäßig von einer Kompromittierung des gesamten IT-Netzwerks inklusive aller damit verbundenen IT-Systeme auszugehen. Darüber hinaus kann es bereits zur Unbrauchbarkeit der IT-Systeme durch Verschlüsselung der darauf gespeicherten Betriebssystem- und/oder Anwendungsdaten gekommen sein.

Denkbar ist dabei die Beseitigung der Schadensursache durch detaillierte Identifizierung von Schadcode auf IT-Systemen und gezielte Bereinigung dieser Systeme. In vielen Fällen dürfte angesichts des zu erwartenden Zeitaufwands bei diesem Vorgehen sowie des verbleibenden Restrisikos einer unerkannten Identifizierung mit Schadsoftware und damit einhergehender späterer Re-Kompromittierung des gesamten IT-Netzwerks eine gesamthafte Wiederherstellung der IT-Systeme aus dem bestenfalls verfügbaren Back-up die präferierte Variante sein.
Zunächst ist deshalb eine Unterstützung bei der Wiederherstellung der Basis-IT-Infrastruktur durch die Bündnismitglieder denkbar. Konkret kann dies die Hilfe bei der Wiederherstellung oder dem Neuaufbau eines Authentifizierungs-Service (z. B. Microsoft Active Directory) durch dafür qualifiziertes IT-Per-

sonal aus dem Bereich des Identity und Access Management bedeuten. Zudem können IT-Netzwerkspezialistinnen und -spezialisten Unterstützung bei der

- Neuinstallation und Konfiguration von Netzwerk-Geräten, z. B Switches, Router, Firewalls,
- Neuinstallation/Konfiguration eines Virtual Private Networks und des Remote Access und
- Wiederherstellung der Festnetztelefonieeinrichtungen leisten.

Ebenso können Bündnismitglieder bei der Installation und Konfiguration der Storage-Systeme und Hypervisor, sowohl on-premise als auch in der Cloud, mit IT-Expertinnen und -Experten aus dem Bereich Hosting/Computing/Storage unterstützen. Diese Tätigkeit bildet die Grundlage für eine nachfolgende Wiederherstellung von Systemen aus vorhandenen Back-ups.
Zuvor können erfahrene Expertinnen und Experten aus den helfenden Unternehmen jedoch gemeinsam mit dem Hilfe suchenden Unternehmen die Güte von vorhandenen Back-ups unter Einbezug der Informationen aus der digitalen Forensik bewerten und Strategien zur effizientesten Datenwiederherstellung entwerfen.
Sinnvoll kann im Weiteren die Inanspruchnahme von Unterstützung der Bündnismitglieder bei der Neuinstallation und Konfiguration spezieller zentraler IT-Dienste sein. Diese umfassen insbesondere System Center Configuration Manager (SCCM), Dynamic Host Configuration Protocol (DHCP) und Domain Name System (DNS).

Einen Schwerpunkt der Arbeitsbelastung in dieser Phase bildet die quantitativ herausfordernde Bereinigung von IT-Endgeräten wie Notebooks und PCs durch Neuinstallation. Gerade diese Tätigkeit ist prädestiniert für eine Unterstützung aus dem Cyber-Bündnis, denn sie erfordert eine große Zahl „helfender Hände“, nicht aber spezielles und damit regelmäßig in geringem Umfang vorhandenes Know-how.

Auf Basis der bereinigten und wiederhergestellten IT-Infrastruktur können dann Unterstützungsleistungen zur Bewältigung des Sicherheitsvorfalls beitragen, etwa in Form von Neuinstallation und Konfiguration von Middleware, ERP-Basis-Diensten und letztlich der benötigen IT-Anwendungen aller Art inklusive der Validierung vorhandener Einstellungen im Sinne einer Qualitätskontrolle vor der Produktivsetzung.

Neben personeller Unterstützung ist grundsätzlich eine materielle Unterstützung durch Bündnismitglieder denkbar. Hierzu zählt beispielsweise die für das Krisenmanagement benötigte Kommunikationsinfrastruktur (z. B. Tenant für Online-Kommunikation und -Kollaboration), „neu“ installierte IT-Hardware (z. B. Notebooks, Festplatten, Netzwerkgeräte).
Der (ggf. gemeinsame) Erwerb, die Verwaltung und die Nutzung von Materialressourcen sind stark abhängig von der gewählten Organisationsform eines Cyber-Bündnisses. Details hierzu sind dem Kapitel „Juristische Aspekte“ zu entnehmen.

3. Juristische Aspekte und Rahmenbedingungen

Die gegenseitige Unterstützung von Unternehmen für Unternehmen bei einem schwerwiegenden Cyber-Angriff hat zahlreiche rechtliche Implikationen, sowohl für die Leitung der in einem Cyber-Bündnis organisierten Unternehmen als auch für deren Mitarbeiterinnen und Mitarbeiter, die die fachliche Unterstützungsleistung erbringen.

Vor dem Hintergrund der Cyber-Bedrohungslage ist die Beschäftigung mit Cybersicherheit eine faktische Pflichtaufgabe für Geschäftsführerinnen und Geschäftsführer. Zusätzlich verpflichten auch rechtliche Vorschriften zu einem dem eigenen Risiko angemessenen Umgang der Unternehmensleitung mit Cybersicherheit – präventiv und reaktiv. Eine aktive Mitgliedschaft in einem Cyber-Bündnis stellt damit einen Baustein unternehmerischer Risikovorsorge dar und demonstriert unmittelbar die Bereitschaft des Managements, entsprechende Vorkehrungen zu treffen. Dadurch werden haftungsrechtliche Risiken der Geschäftsführung gesenkt.

3.1 Haftung

Für helfende Mitarbeiter aus Cyber-Bündnis-Unternehmen stellt sich hingegen die Frage, ob die persönlichen haftungsrechtlichen Risiken durch den eigenen, ggf. freiwilligen Hilfsbeitrag sogar vergrößert werden. Aus juristischer Sicht ist diese Frage abhängig vom konkret gewählten Organisationsmodell eines Cyber-Bündnisses zu beantworten. Insbesondere bei einer unverbindlichen Organisationsform (siehe dazu „Mögliche Cyber-Bündnis-Modelle“) bleibt die Haftung der helfenden Personen jedoch auf die allgemeinen Vorsatz- bzw. Fahrlässigkeitsvorschriften beschränkt und es besteht deshalb kein rechtlicher Regelungsbedarf.

3.2 Arbeitsrecht

Cyber-Bündnismitglieder müssen daneben arbeitsrechtliche Fragen beantworten. Aus juristischer Sicht sind in tatsächlichen Notfällen, zu denen schwerwiegende Cyberangriffe zählen dürften, Ausnahmen von der täglichen Höchstarbeitszeit möglich. Insoweit ist eine Unterstützung eines Cyber-Bündnismitglieds arbeitsrechtlich möglich.
Allerdings könnte der Hilfseinsatz aufgrund geänderter Arbeitsinhalte und Arbeitszeit als Versetzung (vom helfenden Unternehmen) oder als Einstellung (beim Hilfe suchenden Unternehmen) gewertet werden. Kollektivrechtlich würden sich hieraus Mitbestimmungspflichten einer möglicherweise im helfenden und/oder Hilfe suchenden Unternehmen existierenden Arbeitnehmervertretung ergeben.
Diesem Umstand kann jedoch mit verschiedenen rechtlichen und praktischen Instrumenten begegnet werden. So verhindert beispielsweise die Entsendung einer Einsatzleiterin/eines Einsatzleiters jedes helfenden Cyber-Bündnismitglieds die mitbestimmungspflichtige Einstellung der helfenden Personen beim angegriffenen Unternehmen sowie Konflikte

mit dem Arbeitnehmerüberlassungsgesetz, falls disziplinarische Weisungen an die helfenden Personen jeweils nur durch die eigenen Einsatzleitenden erteilt werden.

Darüber hinaus können die Verankerung eines (in örtlicher Hinsicht) weiten Weisungsrechts im Arbeitsvertrag der helfenden Personen sowie Betriebsvereinbarungen mit den Arbeitnehmervertretungen der Cyber-Bündnismitglieder arbeitsrechtliche Hürden abbauen.

3.3 Kartellverbot, Missbrauchs- und Fusionskontrolle

Der Aufbau und der Betrieb von Cyber-Bündnissen ist außerdem auf die Vereinbarkeit von Vorschriften des Kartellverbots, der Missbrauchs- und Fusionskontrolle zu prüfen. Hinsichtlich des Kartellverbots ist vor allem bei der Wahl der Cyber-Bündnismitglieder zu berücksichtigen, dass diese nicht zueinander im Wettbewerb stehen.
Cyber-Bündnisse sind auch mit den Vorschriften zur Missbrauchskontrolle vereinbar. Aus juristischer Sicht ist anzunehmen, dass die Cyber-Bündnismitglieder einzeln als auch in ihrer Gesamtheit keine Marktmacht auf dem relevanten Markt der IT-Dienstleistungen haben. Für Cyber-Bündnisse könnte außerdem eine fusionskontrollrechtliche Anmeldung beim Bundeskartellamt für den Aufbau sowie (ggf. zusätzlich) nachgelagerte strukturelle Veränderung je nach Einzelfall notwendig sein. Im Falle einer Anmeldepflicht ist eine Freigabe durch das Bundeskartellamt zwingend abzuwarten.

3.4 Datenschutz und Informationssicherheit

Schließlich sind auch Datenschutz und Informationssicherheit in Cyber-Bündnissen sicherzustellen. Dies betrifft im Besonderen den Schutz der personenbezogenen Daten von Arbeitnehmerinnen und Arbeitnehmern, aber auch von Kundinnen und Kunden sowie Lieferunternehmen des angegriffenen Unternehmens, die den helfenden Personen der Bündnismitglieder zugänglich werden könnten.

In der Regel ist das betroffene Unternehmen datenschutzrechtlich Verantwortlicher. Die helfenden Cyber-Bündnismitglieder dürften regelmäßig als Auftragsverarbeiter (Art. 28 DSGVO) für das betroffene Unternehmen tätig werden. Dies kann normkonform durch datenschutzrechtliche Vereinbarungen gewährleistet werden, die vorsorglich wechselseitig zwischen den Cyber-Bündnismitgliedern geschlossen werden. Im Hinblick auf den Schutz personenbezogener Daten von Arbeitnehmerinnen und Arbeitnehmern kann die rechtliche Grundlage durch entsprechende Betriebsvereinbarungen bei den einzelnen Cyber-Bündnismitgliedern geschaffen werden.

Darüber hinaus müssen präventiv Vertraulichkeitsvereinbarungen (NDAs) zwischen den beteiligten Unternehmen, aber auch mit den eingesetzten Mitarbeitenden geschlossen werden, um die Weitergabe von unternehmenskritischen (und ggf. auch wettbewerblich relevanten) Informationen (in beide Richtungen) zu unterbinden.

Fazit

Zusammenfassend ist festzuhalten, dass unter Berücksichtigung der dargestellten Rahmenbedingungen keine absoluten juristischen Hinderungsgründe für den Aufbau und Betrieb eines Cyber-Bündnisses zur gegenseitigen Unterstützung von Unternehmen für Unternehmen im Falle eines schwerwiegenden Cyberangriffs vorliegen.
Eine detaillierte Würdigung sämtlicher dieser juristischen Aspekte und Rahmenbedingungen finden Sie als Anlage zum Leitfaden.

4. Organisation

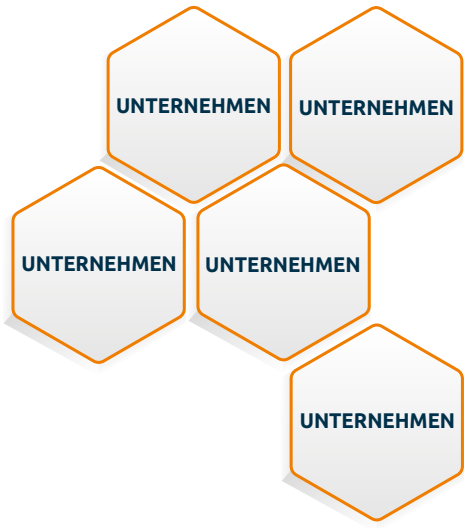
Im folgenden Kapitel werden die organisatorischen Aspekte des Cyber-Bündnisses konkretisiert.

4.1 Struktur und Aufbau eines Cyber-Bündnisses

Organisationsuntersuchungen und Gegebenheiten aus der beruflichen Praxis zeigen immer wieder, dass ein (unabhängig vom Themenfeld) themenorientierter Zusammenschluss eigenständiger Unternehmen zu einem Bündnis aktiv gesteuert werden muss, um nach der Gründung nicht an Bedeutung zu verlieren. Hinzu kommt, dass die Steuerungsaufwände mit zunehmender Größe des Bündnisses erheblich zunehmen. Daher sprechen sich die Verfasserinnen und Verfasser des vorliegenden Leitfadens für eine dezentrale organisatorische Gliederung von Cyber-Bündnissen aus.

Dezentrale Cyber-Bündnisse als Zusammenschluss von mehreren Unternehmen stellen jeweils eine funktionsfähige und in sich geschlossene Einheit im Sinne einer Netzwerkwabe dar, die sich im Bedarfsfall gegenseitig auf Basis selbst definierter Regelungen und Vereinbarungen unterstützen. Auf diese Weise wird sichergestellt, dass die Steuerungsaufwände der einzelnen Cyber-Bündnisse überschaubar bleiben und dennoch ein spürbarer Mehrwert im Bedarfsfall entsteht.

Die einzelnen Cyber-Bündnisse agieren jedoch nicht im leeren Raum. Es wird davon ausgegangen, dass im Laufe der Zeit mehrere unabhängige Netzwerkwaben entstehen. Sollte ein Cybervorfall die Leistungsfähigkeit eines einzelnen Cyber-Bündnisses übersteigen, könnte in diesem Falle bei anderen Cyber-Bündnissen um weitere Unterstützung gebeten werden.



Die Vorteile der dezentralen Wabenstruktur der Cyber-Bündnisse liegen auf der Hand:

1. Beschleunigung des operativen Aufbaus eines Cyber-Bündnisses durch geringe initiale Hürden
2. Schaffung homogener und individuell angepasster Regeln, Prozesse und Strukturen innerhalb der einzelnen Cyber-Bündnisse
3. Reduzierung der Steuerungs- und Managementaufwände durch eine begrenzte Zahl an teilnehmenden Organisationen
4. Individuelle Aufnahmekriterien stellen den praktischen Mehrwert der Unterstützung sicher
5. Begünstigung heterogener Entwicklung und damit einhergehender Vielfalt zwischen den einzelnen Waben zur mittel- und langfristigen Identifizierung von Best Practices
6. Minimierung kartellrechtlicher Hürden

Die Wabenstruktur erscheint nicht nur aus praktischen, sondern auch aus verschiedenen rechtlichen Erwägungen sinnvoll. Weitere Details sind dem Kapitel „Juristische Aspekte“ zu entnehmen.

4.2 Kriterien für die Aufnahme in ein Cyber-Bündnis

Die Aufnahmekriterien in ein bestehendes oder neu zu gründendes Cyber-Bündnis sollten sorgfältig und klar definiert werden.
Für eine erste Orientierung kann es hilfreich sein, folgende Aspekte als relevante Aufnahmekriterien in Erwägung zu ziehen:

ÜBERGEORDNETE KRITERIEN	EXEMPLARISCHE AUSGESTALTUNG
Regionale Bezüge	Es können nur Mitglieder in das Cyber-Bündnis aufgenommen werden, deren IT-Headquarter im Umkreis von 100 km um Stuttgart liegt.
Branchenbezüge	Es können nur Mitglieder in das Cyber-Bündnis aufgenommen werden, die im Bereich der Baubranche tätig sind. Gleichzeitig sollten die Mitglieder aus rechtlichen Gründen jedoch nicht im direkten Wettbewerb zueinander stehen.
Unternehmensgröße	Es können nur Mitglieder in das Cyber-Bündnis aufgenommen werden, deren Unternehmen nicht weniger als 1.000 Mitarbeiter und nicht mehr als 5.000 Mitarbeiter haben.
Budgetbezüge	Es können nur Mitglieder in das Cyber-Bündnis aufgenommen werden, die bereit sind, für die Arbeit im Cyber-Bündnis 5.000 Euro (netto) pro Jahr bereitzustellen.
Sonstige Kriterien	- Anzahl der angestellten IT-Mitarbeitenden - Ähnlichkeiten in Aufbau und Architektur der IT - ...

Der Beschluss für die Aufnahme in ein bestehendes Cyber-Bündnis sollte durch eine Abstimmung der Mitglieder in einem regelmäßig tagenden Entscheidungsgremium gefasst und festgehalten werden. Entscheidungen sollten die mehrheitliche Zustimmung der Mitglieder erfordern, wobei jedes Mitgliedsunternehmen eine Stimme hat („auf Augenhöhe").

Jedes Bündnismitglied kann den Austritt für sich selbst beschließen. Das Cyber-Bündnis kann durch mehrheitlichen Beschluss den Ausschluss eines Mitglieds beschließen, wenn beispielsweise übergeordnete Kriterien für ein Mitglied nicht mehr zutreffend sind.

4.3 Budgetausstattung

Die Bündnismitglieder können sich – insbesondere in verbindlicher Organisationsform – verpflichten, ein gewisses Budget zur Verfügung zu stellen, um die Arbeit des Bündnisses aufrecht erhalten zu können. Hierbei sind beispielsweise Aufwände für die Vorbereitung und das Vorhalten von Ressourcen sowie regelmäßigen Austausch und Abstimmungen der Bündnismitglieder vorzusehen. Beispiele für geteilte Ressourcen können sein:

- IT-Forensik-Soft- und -Hardware
- Netzwerkhardware
- Notebooks
- Schulungsmaterialien

4.4 Incentivierung

Um das Bündnis einsatzfähig zu halten, kann ein gewisser Beitrag durch jedes Mitglied eingefordert werden. Jeder Einsatz der Bündnismitglieder für die Reaktion auf einen schwerwiegenden Cyberangriff erfordert die Bereitstellung von IT-Fachkräften und ggf. Hard- und Software der Mitglieder. Dieser Einsatz geschieht einerseits im Sinne eines gegenseitigen Schutzes und bindet andererseits sehr kurzfristig hoch qualifizierte Ressourcen.

Hierbei ist zu beachten, dass sich nicht jedes Mitglied dem gleichen Risiko ausgesetzt fühlt und auch nicht jedes Mitgliedsunternehmen gleich viel für die Gefahrenabwehr investiert. Ferner ist zu berücksichtigen, dass nicht jedes Mitglied die gleichen Ressourcen bereitstellen kann. Die genannten Punkte verdeutlichen, dass eine finanzielle Incentivierung und somit eine faire Leistungsverrechnung notwendig sind.

Für die Umsetzung einer fairen Leistungsverrechnung sollte innerhalb jedes Bündnisses eine einheitliche Definition zur Gründung festgelegt und ggf. auf Basis einer mehrheitlichen Entscheidung der Mitglieder überarbeitet werden.
Die Leistungsverrechnung sollte idealerweise den zeitlichen Aufwand berücksichtigen, der tatsächlich angefallen ist, und mit einem Verrechnungssatz multipliziert werden. Der Verrechnungssatz sollte hierbei so nahe wie möglich bei den realistischen Selbstkosten liegen. Zur vereinfachten Handhabung und im Sinne einer fairen Verrechnung sollte ein gemeinsamer Satz ggf. am durchschnittlichen internen Verrechnungssatz der Mitgliedsunternehmen orientiert sein.

4.5 Mögliche Cyber-Bündnis-Modelle

Aus organisatorisch-praktischer Sicht ist es für ein effizientes Cyber-Bündnis wichtig, das richtige Maß zwischen organisatorischem und finanziellem Aufwand (sowohl in der Gründungs- als auch in der Betriebsphase) einerseits sowie Verbindlichkeit und Verlässlichkeit hinsichtlich der Hilfeleistungsbereitschaft im Notfall andererseits zu finden.

Es ist die wesentliche Aufgabe jedes Unternehmens bzw. der Unternehmensleitung, die Vor- und Nachteile im Einzelfall abzuwägen, um den unternehmerischen Sorgfaltspflichten gerecht zu werden (zur Compliance s. o. unter „Juristische Aspekte und Rahmenbedingungen“). Grundsätzlich lässt sich festhalten:

- Eine lose Organisation führt zu wenig Verbindlichkeit und Verlässlichkeit hinsichtlich der Hilfeleistung.
- Je höher der Organisationsgrad, desto höher ist der Grad an Verbindlichkeit und Verlässlichkeit der Hilfeleistung.
- Ohne Verbindlichkeit und Verlässlichkeit hinsichtlich der Hilfeleistung können die Ziele eines Cyber-Bündnisses im Notfall nicht erreicht werden.
- Je geringer der Grad an Verbindlichkeit und Verlässlichkeit der Hilfeleistung, desto höher ist das Risiko für Unternehmen, im Notfall keine adäquate Hilfeleistung zu erhalten.

In diesem Leitfaden werden drei mögliche Cyber-Bündnis-Modelle im Spannungsfeld zwischen Verlässlichkeit und Organisationsaufwand vorgeschlagen. Alle drei Modelle sind grundsätzlich rechtskonform umsetzbar.

1: „Handschlag“-Vereinbarung

Das Modell „Handschlag“ zeichnet sich durch sehr geringen Organisations- und Kooperationsaufwand aus. Rechtlich gesehen basiert es – je nach konkreter Ausgestaltung im Einzelfall – auf einem reinen Gefälligkeitsverhältnis oder einer Gesellschaft bürgerlichen Rechts.

sehr geringer Organisations- und Kooperationsaufwand, rechtlich reines Gefälligkeitsverhältnis oder eine Gesellschaft bürgerlichen Rechts

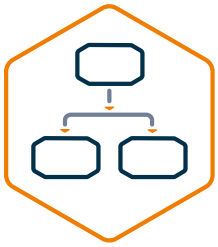
2: „Handschlag plus Standard- und Musterverträge“

Das Modell „Handschlag plus Standard- und Musterverträge“ ist bei weiterhin geringem Organisationsaufwand bereits verfestigter. Die beabsichtigte Erfüllung rechtlicher Mindestanforderungen und die Erhöhung der Verlässlichkeit gelingen durch die Vereinbarung von Musterverträgen.

geringer Organisationsaufwand, stärkere Bindung, rechtliche Mindestanforderungen, erhöhte Verlässlichkeit durch Musterverträge

3: Organisation in verbindlicher Form

Das Modell „Eigenständige Cyber-Bündnis-Organisation“ zeichnet sich durch eine selbstständige und verbindliche Organisationsstruktur aus, die jedoch mit hohem Organisationsaufwand verbunden ist. Eine detaillierte Darstellung der o. g. Cyber-Bündnis-Modelle mit den jeweiligen Vor- und Nachteilen aus juristischer Perspektive finden Sie als Anlage zum Leitfaden.



selbstständige und verbindliche Organisationsstruktur, hoher Organisationsaufwand

Übersicht Anhang

Anhang 1: Organisation und juristische Aspekte

Anhang 2: Musterverträge[1]

- Arbeitsvertragsklauseln zum Einsatz bei kritischen Vorfällen einschließlich Datenschutzinformationen
- Belehrung zur Geheimhaltung (Beschäftigte)
- Betriebsvereinbarung über den Einsatz von Dritten im Betrieb bei Cyberattacken
- Betriebsvereinbarung über den Einsatz von Mitarbeiterinnen und Mitarbeitern bei Dritten zur Abwehr von kritischen Vorfällen und Attacken
- Betriebsvereinbarung zur Datennutzung im Falle eines kritischen Vorfalls
- Betriebsvereinbarung zur Lage und Dauer der Arbeitszeit bei kritischen Vorfällen
- Geheimhaltungsvereinbarung (Unternehmen)
- Verpflichtung auf das Datengeheimnis (Beschäftigte)
- Vereinbarung über die datenschutzrechtliche Auftragsverarbeitung
- Vereinbarung über die gemeinsame datenschutzrechtliche Verantwortlichkeit

Die Musterverträge stehen online auf der Website der Allianz Industrie 4.0 Baden-Württemberg zum Abruf und Download zur Verfügung.

[1] Bei den gelisteten Verträgen und Texten handelt es sich ausdrücklich um **Muster**, die den Cyber-Bündnis-Mitgliedern einen Eindruck über die empfohlenen bzw. möglichen Regelungsinhalte geben sollen, jedoch zwingend der **Anpassung auf den jeweiligen Einzelfall** unter Berücksichtigung der Besonderheiten der Mitgliedsunternehmen bedürfen.

Projektbeteiligte

Dieser Leitfaden entstand in der Projektgruppe „Leitfaden Cyber-Bündnis“ der Allianz Industrie 4.0 Baden-Württemberg.

Dominik Helble
Leiter der Projektgruppe

Leitung Cyber Security,
Festo SE & Co. KG

Jana Eiser-Mauthner
Projektleiterin der
Allianz Industrie 4.0
Baden-Württemberg,
VDMA e. V.
Baden-Württemberg

Prof. Dr Michael Auer, Steinbeis-Stiftung für Wirtschaftsförderung (StW)

Andreas Behncke, DÜRR Group

Josef Flügel, Lenze SE

Timo Herzog, Eberspächer Climate Control Systems GmbH & Co. KG

Dr. Moritz Huber, smartSEC GmbH

Lukas Linke, Alfred Kärcher SE & Co. KG

Yannick Mayer, Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA

Simon Meraner, Zoi TechCon GmbH

Henrik Mündörfer, Dieffenbacher GmbH Maschinen- und Anlagenbau

Oliver Ortlieb, Carl Zeiss AG

Dr. rer. pol. Dipl.-Inf. Heiko Roßnagel, Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO

Lukas Schleicher, Allianz Industrie 4.0 Baden-Württemberg

Uta Schmidt, MESTO Spritzenfabrik Ernst Stockburger GmbH

Wolfgang Schuster, WITTENSTEIN SE

Steffen Zimmermann, VDMA e. V. Competence Center Industrial Security e. V.

In Kooperation mit:

GvW Graf von Westphalen | Rechtsanwälte Steuerberater Partnerschaft mbB
Ulmenstraße 23-25
60325 Frankfurt a. M.

Datenschutz und Cybersecurity
Dr. Michael Herold, M.C.L., m.herold@gvw.com, T +49 69 707970-186
Stephan Menzemer, s.menzemer@gvw.com, T +49 69 707970-186

IT Compliance und Risk
Carsten Beisheim, c.beisheim@gvw.com, T +49 211 56615-166

Arbeitsrecht
Christof Kleinmann, c.kleinmann@gvw.com, T +49 69 707970-0

Kartellrecht
Christian Kusulis, c.kusulis@gvw.com, T +49 69 707970-136

Steuerrecht
Dr. Michael Engel , m.engel@gvw.com, T +49 69 707970-117

Mit Unterstützung von:

Baden-Württemberg
MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND TOURISMUS

VDMA

Impressum

Allianz Industrie 4.0 Baden-Württemberg
beim VDMA e. V. Baden-Württemberg
Kronenstr. 3
70173 Stuttgart
Tel.: +49 711 22801-20
E-Mail: info@i40-bw.de
Internet: www.i40-bw.de

Kontakt
Jana Eiser-Mauthner
Projektleiterin Allianz Industrie 4.0 Baden-Württemberg
Tel.: +49 711 22801-27
E-Mail: jana.eiser-mauthner@vdma.org

Design und Layout
fuchsconcepts
Esslinger Straße 87
70734 Fellbach

Satz und Druck
burger Print & Medien GmbH
Furtstraße 2/1
75242 Neuhausen

Erscheinungsjahr
2023

Allianz Industrie 4.0 Baden-Württemberg
VDMA e. V. Baden-Württemberg
Kronenstraße 3
70173 Stuttgart

Tel.: +49 711 22801-20
E-Mail: info@i40-bw.de
Internet: www.i40-bw.de

Gefördert durch:

Baden-Württemberg
MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND TOURISMUS

Mit Unterstützung von:

VDMA