

In Kooperation mit  
dem Landeskriminalamt  
Baden-Württemberg

CYBER

SECURITY

RISK

REPORT

21



Der Cyber-Security-Risk-Report 2021 und die dazugehörige Executive Summary wurden herausgegeben von: MHP Management- und IT-Beratung GmbH in Kooperation mit dem Landeskriminalamt Baden-Württemberg.



**Andreas Henkel**  
Associated Partner  
MHP Focus Topic  
Lead Cyber Security



**Andreas Stenger**  
Präsident  
Landeskriminalamt  
Baden-Württemberg

Im Januar 2022.

**Alle Rechte vorbehalten!**

Vervielfältigung, Mikroverfilmung, die Einspeicherung und Verarbeitung in elektronischen Medien sind ohne Zustimmung der Herausgeber nicht gestattet. Die Inhalte entsprechen dem Kenntnisstand der Autor\*innen zum Zeitpunkt der Veröffentlichung. Für die Lösung einschlägiger Probleme greifen Sie bitte auf die in der Publikation angegebenen Quellen zurück oder wenden sich an die genannten Ansprechpartner. Meinungsbeiträge geben die Auffassung der einzelnen Autor\*innen wieder. In den Grafiken kann es zu Rundungsdifferenzen kommen.

# VORWORT

Sehr geehrte Leserinnen und Leser,

die zunehmende Digitalisierung bietet für die Mehrheit der Unternehmen in Deutschland zahlreiche neue und einzigartige Chancen. Regelmäßig und in immer kürzer werdenden Abständen zeigt sich aber auch, dass eine erfolgreiche digitale Transformation ebenso Risiken mit sich bringen kann. Unternehmen, öffentliche Einrichtungen, nichtstaatliche Organisationen sowie Privatpersonen sind immer wieder Cyber-Angriffen ausgesetzt. Die Bedrohungslage durch Attacken von Hacker\*innen in ihren verschiedenen Ausführungen nimmt stetig zu. Das Ziel sind Daten, die in einer digitalen Welt nicht nur ein wertvolles, sondern auch sensibles Gut repräsentieren.

Systematisch ausgenutzt werden von den Angreifenden etliche bestehende Schwachstellen – unter anderem veraltete Soft- oder Hardware, mangelnde Sicherheitsstandards oder menschliches Fehlverhalten. Ein erfolgreicher Cyber-Angriff kann für alle Beteiligten schnell zu monetären und nicht monetären Schäden – etwa einem Reputationsverlust – führen und auch rechtliche Folgen nach sich ziehen. Die Auswirkungen sind dabei nicht auf die attackierten Unternehmen begrenzt, sondern können auch Drittparteien entlang der gesamten Wertschöpfungskette oder sogar die gesamte Gesellschaft betreffen.

Aufgrund von steigenden und diversen Bedrohungslagen stellen Cyber-Angriffe zunehmend ein strategisches Risiko dar. Die umfassende Absicherung mit geeigneten und kontinuierlich zu validierenden Schutzmaßnahmen gegen Zugriffe von Kriminellen im Cyber-Raum ist daher mittlerweile eines der zentralen Handlungsfelder

von Unternehmen. Doch wie gut sind Unternehmen in Deutschland derzeit dieser anspruchsvollen Aufgabe gewachsen?

Genau darauf wollen die MHP Management- und IT-Beratung GmbH in Kooperation mit dem Landeskriminalamt Baden-Württemberg im vorliegenden Cyber-Security-Risk-Report mithilfe qualitativer Experteninterviews und einer breit gefächerten quantitativen Befragung Antworten geben.

Ausgehend von den Antworten der Experten und der insgesamt 314 Teilnehmenden aus unterschiedlichsten Unternehmen und Wirtschaftsbereichen wurden Erkenntnisse zu den etablierten Cyber-Security-Maßnahmen und den zukünftigen Herausforderungen identifiziert. Daraus haben die Autor\*innen Optimierungspotenziale abgeleitet, um abschließend spezifische Handlungsempfehlungen zu definieren. Mit dieser umfassenden Betrachtung sollen das Risikobewusstsein gesteigert und gleichzeitig praktische Impulse für eine bessere Prävention gegeben werden.

An dieser Stelle gilt ein großer Dank den Cyber-Security-Experten, die sich trotz ihres fordernden Arbeitsalltags Zeit genommen haben, ihre Erfahrung und Einschätzungen zu teilen.

Wir wünschen Ihnen interessante Einblicke, Erkenntnisse und viel Spaß beim Lesen des Cyber-Security-Reports.

# INHALTS- VERZEICHNIS

<b>Vorwort</b>	<b>4</b>
.....	
<b>Schlüsselergebnisse</b>	<b>7</b>
.....	
<b>1.0 Cyber-Security-Risk-Report</b>	<b>8</b>
1.1 Inhalt	8
1.2 Experteninterviews	9
1.3 Teilnehmende	10
1.4 Auswertungsmethodik	11
.....	
<b>2.0 Ergebnisse des Reports</b>	<b>14</b>
2.1 Bedrohungsszenarien	14
Experteninterview Landeskriminalamt Baden-Württemberg	<b>23</b>
2.2 Reaktive Vorfallsbehandlung	32
Experteninterview Siemens AG	<b>39</b>
2.3 Präventive Risikobehandlung	46
.....	
<b>3.0 Handlungsempfehlungen</b>	<b>52</b>
Handlungsempfehlungen im Detail	54
.....	
<b>4.0 Fazit und Ausblick</b>	<b>58</b>
Ansprechpartner & Autor*innen	60

1

Je größer ein Unternehmen ist, desto ausgeprägter die Bereitschaft, Polizeibehörden in die Aufklärung von Cyber-Angriffen einzubinden.

Kleine Unternehmen ziehen seltener Polizeibehörden hinzu, wodurch viele Cyber-Angriffe nicht erfasst werden.

3

Analysen von IT-sicherheitsrelevanten Risiken sind in Unternehmen nur fragmentarisch vorhanden.

Fehlende Aspekte in der Risikoidentifikation verhindern häufig eine umfassende Risikobetrachtung.

4

Bei jedem zweiten Unternehmen waren Kommunikationsdaten – beispielsweise Kontaktdaten und Inhalte von E-Mails – im Rahmen eines Angriffs betroffen. Erfreulicherweise wird eine hohe Aufmerksamkeit auf den Schutz dieser Daten gelegt.

Der Schutz von Daten zur Unternehmensstrategie dagegen steht nicht im Fokus. Dabei sind diese Daten bei einem Drittel der Angriffe betroffen.

2

Die zentrale IT-Abteilung ist hauptverantwortlich für die Identifikation von Cyber-Security-Risiken. Unterstützt wird sie von der Geschäftsführungsebene.

Kleine Unternehmen legen die Verantwortung für den Umgang mit Cyber-Security-Risiken mehrheitlich in die Hände der Geschäftsführung, die Unterstützung von externen Dienstleistern erhält.

## SCHLÜSSEL- ERGEBNISSE

6

Grundlegende präventive Maßnahmen wie beispielsweise Passwortsicherheit, Malwareschutz und Back-ups werden mehrheitlich von Unternehmen eingesetzt.

Maßnahmen zur Passwortsicherheit und eine Multi-Faktor-Authentifizierung sind derzeit jedoch nicht 100 Prozent durchgängig bei allen Unternehmen implementiert.

5

Die Mehrheit der Unternehmen setzt die gängigsten präventiven Maßnahmen ein.

Back-up-Strategien existieren zwar in vielen Unternehmen, ihre Wirksamkeit ist allerdings stark von der technischen Umsetzung abhängig.

8

Bei jedem dritten Angriff kommt Social Engineering zum Einsatz.

Mehr als ein Drittel der befragten Unternehmen bindet das Thema Social Engineering allerdings nicht in ihre Schulungen ein.

7

Eine mangelhafte Sensibilisierung und Unachtsamkeit der Mitarbeitenden stellen in einem Viertel der Fälle den Angriffsvektor dar.

Dementsprechend ist positiv anzumerken, dass die Awareness für Cyber Security bei einem Großteil der Unternehmen auf allen Hierarchieebenen durch Schulungen erhöht wird.

## 1.1 Inhalte

Um einen ganzheitlichen und gut strukturierten Eindruck zur aktuellen Lage der Cyber Security beziehungsweise IT-Sicherheit (fortfolgend werden die beiden Begriffe synonym verwendet) in Deutschland zu erhalten, wurde der Cyber-Security-Risk-Report inhaltlich in drei Cluster gegliedert:

- **Bedrohungsszenarien**  
Akteure sowie Angriffswerkzeuge und -pfade zur Ableitung möglicher Bedrohungen
- **Reaktive Vorfallsbehandlung**  
Relevante Prozesse und Tätigkeiten zur optimalen Reaktion auf einen IT-sicherheitsrelevanten Vorfall
- **Präventive Risikobehandlung**  
Technische und organisatorische Maßnahmen zur Minimierung von IT-sicherheitsrelevanten Risiken

Daten zu den drei Clustern wurden mithilfe einer anonymen Befragung erhoben.



## 1.2 Experteninterviews

Der Cyber-Security-Risk-Report enthält neben der Auswertung der Umfrageergebnisse Interviews mit Experten aus wirtschaftlichem und öffentlichem Sektor.

Die Interviewpartner wurden mithilfe von teilstrukturierten Leitfäden nach ihrer persönlichen Einschätzung sowie ihrer Erfahrung zum aktuellen Entwicklungsstand der Cyber-Security-Thematik befragt. Durch die individuelle Schwerpunktsetzung konnten komplexe Zusammenhänge detailliert dargestellt und Entscheidungsprozesse spezifisch erläutert werden.

Folgende Experten wurden im Rahmen dieses Reports befragt:

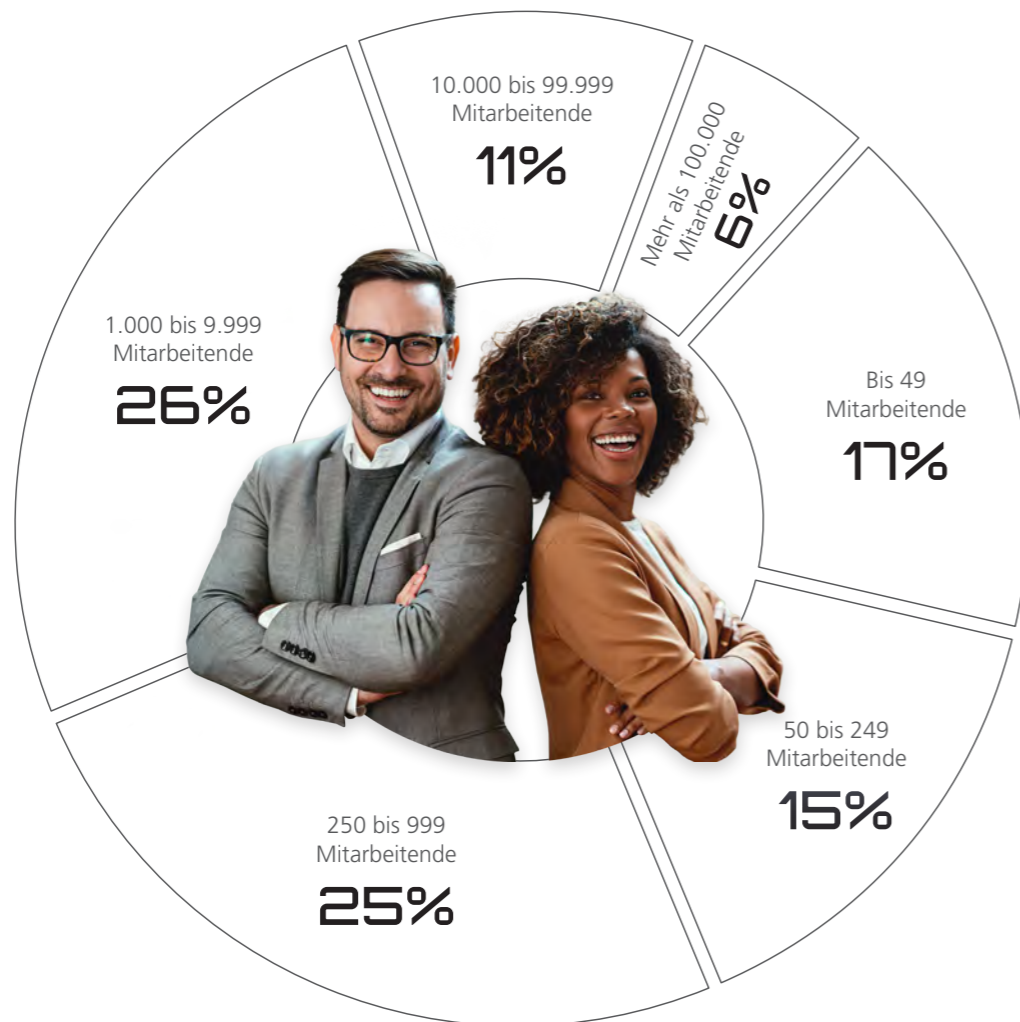
- **Rudolf Näher**  
Leiter der Zentralen Ansprechstelle Cybercrime, Landeskriminalamt Baden-Württemberg
- **Bernd Bauer**  
Head of Protection and Consulting Services, Siemens AG

### 1.3 Teilnehmende

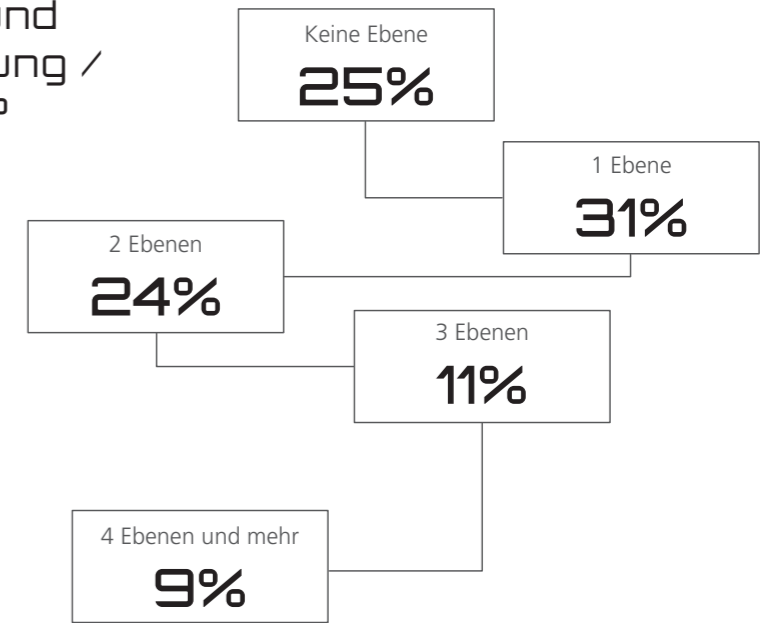
Zur Erhebung des aktuellen Sachstands und der Relevanz der Cyber Security innerhalb der deutschen Wirtschaft wurde zwischen dem 26. Mai und dem 6. September 2021 eine anonyme teilnehmeroffene Online-Befragung durchgeführt. Die nachfolgenden Ergebnisse des Cyber-Security-Risk-Reports beruhen auf den Antworten von 314 Teilnehmenden verschiedener Unterneh-

men und Hierarchieebenen. Nicht alle Befragten haben den Fragebogen komplett ausgefüllt. Die Verteilung der Teilnehmenden nach Unternehmensgrößen und Wirtschaftsbereichen sowie die Differenzierung nach deren Hierarchieebenen sind den nachfolgenden Abbildungen zu entnehmen.

#### Wie viele Mitarbeiter/innen sind in Ihrem Unternehmen beschäftigt?



#### Wie viele Hierarchieebenen liegen zwischen Ihnen und der Geschäftsführung / dem Vorstand?



### 1.4 Auswertungsmethodik

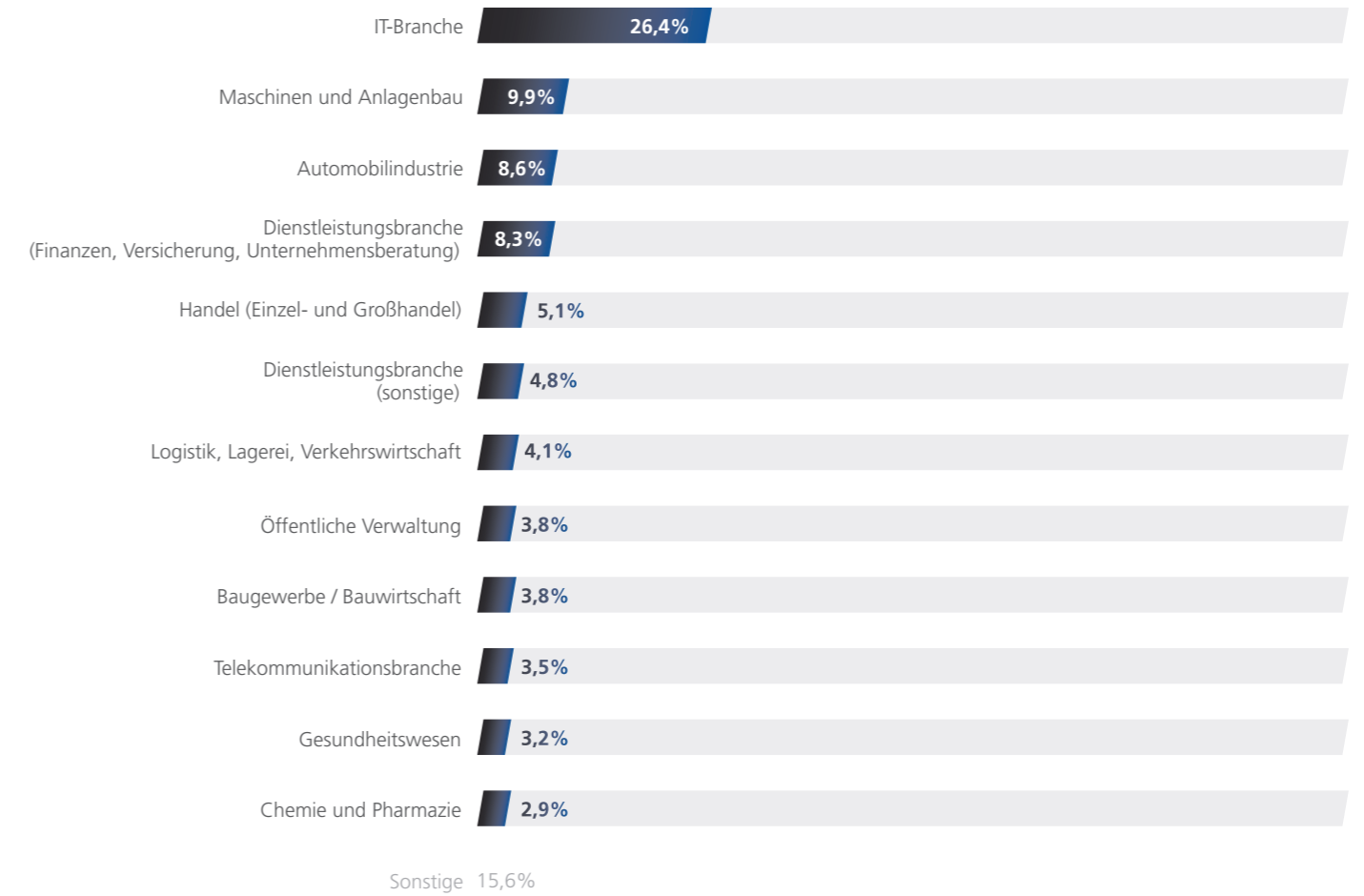
Bei der Online-Befragung wurden Antwortschemata im Multiple- und im Single-Choice-Design verwendet. Die Ergebnisse wurden anhand unterschiedlicher Merkmale der Teilnehmenden und ihrer Unternehmen verglichen: Zum einen nach Unternehmensgröße (klein ( $\leq 49$  Mitarbeitende), mittel ( $\geq 50$  bis  $\leq 999$  Mitarbeitende) und groß ( $\geq 1.000$  Mitarbeitende)), zum anderen nach Wirtschaftsbereich.

eine entsprechende Frage im Single-Choice-Design verwendet. Konkret wurde gefragt, ob innerhalb der vergangenen zwei Jahre ein IT-sicherheitsrelevanter Vorfall mit daraus resultierendem Schadenseintritt stattgefunden hat. Die betroffenen Unternehmen beantworteten zusätzlich sieben angriffsspezifische Fragen.

**Erhebung und Auswertung der Antworten erfolgten anonym.**

Damit Unternehmen, die bereits von IT-sicherheitsrelevanten Vorfällen betroffen waren, differenziert betrachtet werden konnten, wurde zu Beginn der Online-Befragung

## In welchem Wirtschaftsbereich ist Ihr Unternehmen tätig?



## 2.1 Bedrohungsszenarien

### IT-sicherheits- relevanter Vorfall

Ein **IT-sicherheitsrelevanter Vorfall** ist eine bestehende oder unmittelbar bevorstehende Beeinträchtigung des definierten Sicherheitsniveaus eines Unternehmens beziehungsweise einer Institution. Bei einem solchen Ereignis werden Aspekte wie Vertraulichkeit, Integrität und Verfügbarkeit der Daten beziehungsweise Systeme beeinträchtigt. Die Folgen können beispielsweise ausgespähte, manipulierte, beschädigte oder gelöschte Informationen einer Organisation sein.

**ERGEBNISSE**

**DES**

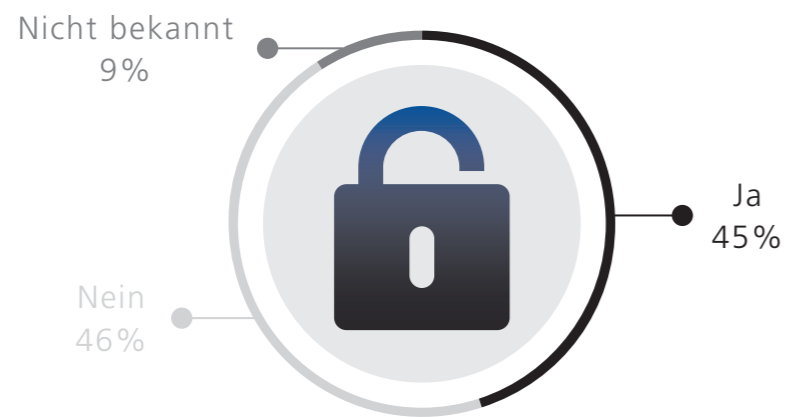
**REPORTS**

**2.0**

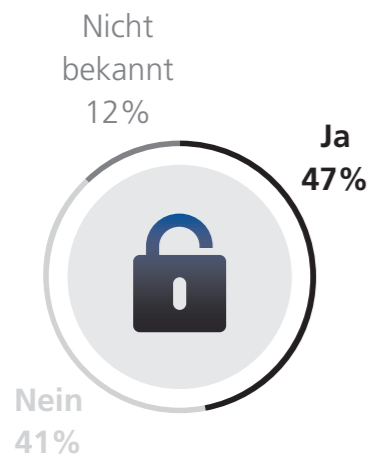
Unter **Bedrohungsszenarien** werden identifizierte potenzielle Angriffsakteure, Angriffswerkzeuge und Angriffspfade verstanden. Das Ziel ist es, Bedrohungen hinsichtlich der geschäftskritischen Aktivitäten und der daraus resultierenden Sicherheitslücken zu bewerten.



## War Ihr Unternehmen innerhalb der letzten 2 Jahre von IT-sicherheitsrelevanten Vorfällen mit resultierendem Schadenseintritt betroffen?



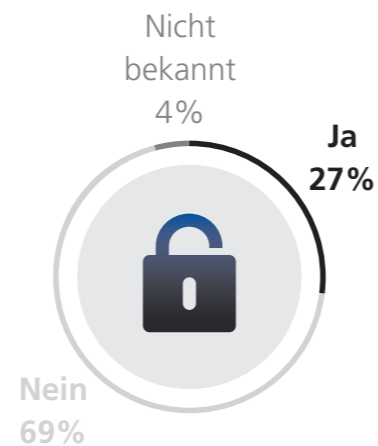
### Große Unternehmen



### Mittlere Unternehmen



### Kleine Unternehmen



### Bedrohungslage in Deutschland: Jedes zweite Unternehmen betroffen

Entsprechend der steigenden gesellschaftlichen, politischen und wirtschaftlichen Wahrnehmung erhält die Cyber-Security-Thematik im Rahmen der Digitalisierung zunehmend eine bedeutendere Rolle. Zu der verstärkten öffentlichen Aufmerksamkeit haben verschiedene schwerwiegende Fälle beigetragen. Tatsächlich sind Cyber-Attacken mittlerweile eine alltägliche Bedrohung. So gibt knapp die Hälfte (45 %) der von uns befragten Personen an, ihr Unternehmen sei in den zurückliegenden zwei Jahren durch einen IT-sicherheitsrelevanten Vorfall geschädigt worden.

Es wird aber davon ausgegangen, dass der Anteil aufgrund nicht bekannter Angriffe höher ist. Eine mögliche Dunkelziffer ergibt sich zum einen dadurch, dass der Erfahrung nach nicht alle Angriffe von den Unternehmen erkannt werden. Angreifende finden oftmals deutlich vor der Erkennung des Vorfalls Zugang zu den Systemen. Der offensichtliche Schaden in Form von beispielsweise verschlüsselten Daten oder Lösegeldforderungen erfolgt erst zu einem späteren Zeitpunkt. Zum anderen ist denkbar, dass trotz Anonymität nicht alle Teilnehmenden angegeben haben, dass bereits ein Vorfall stattgefunden hat.

### Deutlich weniger Angriffe bei kleinen Unternehmen

Werden die IT-sicherheitsrelevanten Vorfälle auf die Unternehmensgröße bezogen, sind deutliche Unterschiede zu erkennen: Lediglich 27 Prozent der Befragten aus kleinen Unternehmen geben an, dass sie bereits Ziel eines Cyber-Angriffs waren und daraus ein Schaden für das Unternehmen entstanden ist. Bei mittleren Unternehmen sind es 50 Prozent, bei großen Unternehmen 47 Prozent.

Als Erklärung dafür, dass kleine Unternehmen signifikant seltener betroffen sind, kommen verschiedene Aspekte infrage: Kleine Unternehmen stellen aufgrund ihrer geringeren Anzahl an digitalen Assets für die meisten Angreifenden ein vermeintlich weniger attraktives oder bekanntes Angriffsziel dar. Des Weiteren fehlen besonders in kleinen Unternehmen häufig die Ressourcen, die notwen-

digen Kompetenzen und die entsprechende Infrastruktur für eine zuverlässige Vorfallerkennung. Cyber-Attacken finden also möglicherweise statt, werden aber seltener erkannt.

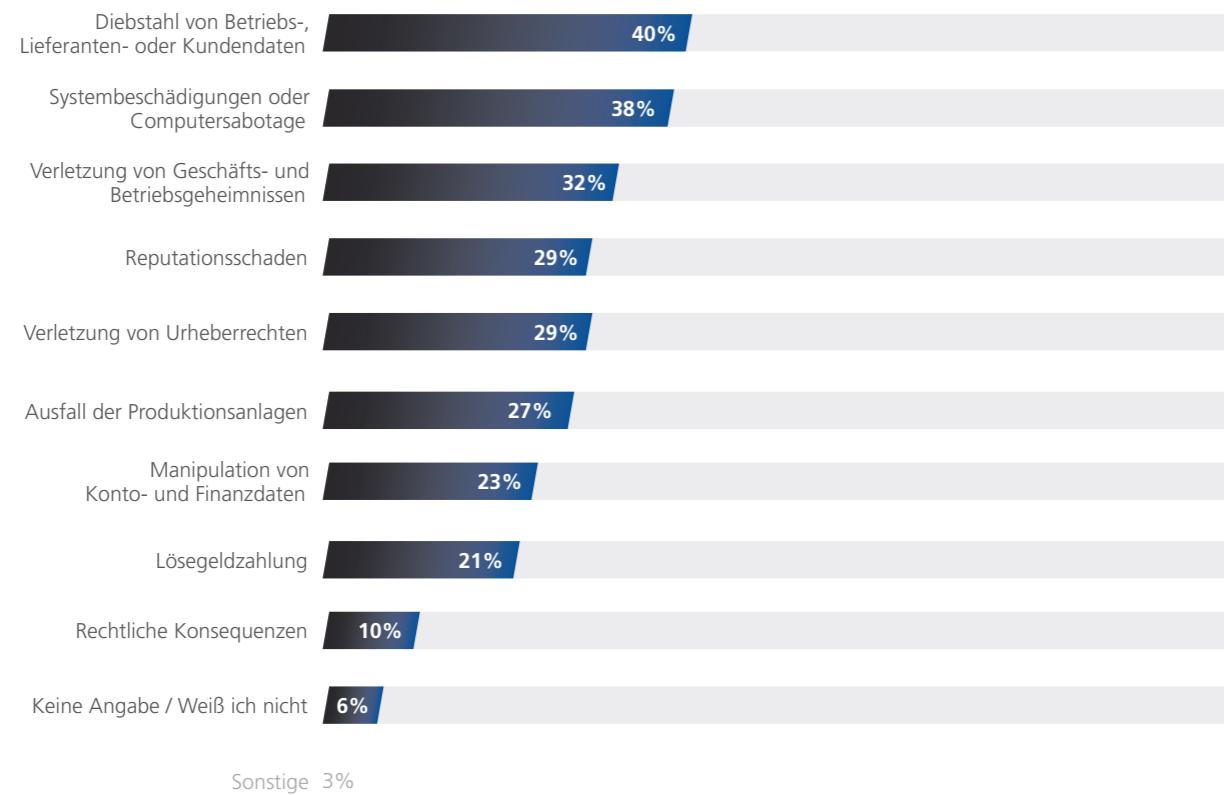
### Weniger Angriffe bei Wirtschaftsbereichen mit physischen Assets

Auch der Blick auf die verschiedenen Wirtschaftsbereiche legt nahe, dass die Anzahl der digitalen Assets ein zentraler Faktor ist: Wirtschaftsbereiche, für die angenommen werden kann, dass eher wenige digitale Assets vorhanden sind, sind seltener von Angriffen betroffen. Wirtschaftsbereiche mit einer erwartungsgemäß höheren Anzahl an digitalen Assets erleben häufiger Cyber-Attacken. Im Baugewerbe etwa liegt der Anteil der Unternehmen, die bereits einen IT-sicherheitsrelevanten Vorfall erlebt haben, mit 25 Prozent deutlich unter dem Durchschnitt. In der IT-Branche berichten 52 Prozent der Unternehmen von solchen Vorfällen, in der Telekommunikationsbranche sogar 82 Prozent der Unternehmen. Es könnte angenommen werden, dass in diesem Bereich ein höherer Digitalisierungsgrad vorhanden ist, wodurch mehr potenzielle Angriffsflächen bestehen. Hinzu kommt, dass in diesen Wirtschaftsbereichen eine höhere Erkennungsrate von IT-sicherheitsrelevanten Angriffen zu erwarten ist.

Mit 89 Prozent ist die Quote bei Unternehmen im Wirtschaftsbereich Chemie und Pharmazie ebenfalls überdurchschnittlich hoch. Das liegt vermutlich daran, dass diese überaus attraktive Assets und Daten für Angreifende aufweisen und dadurch ein interessantes Ziel sind. Auch hier kann, wie in der IT- und Telekommunikationsbranche, davon ausgegangen werden, dass entsprechende Erkennungsmechanismen umfangreich etabliert sind. Unternehmen der Automobilbranche weisen mit 44 Prozent eine durchschnittliche Quote auf. Allerdings ist angesichts der zunehmenden Vernetzung von Fahrzeugen künftig eine höhere Zahl an digitalen Schnittstellen zu erwarten. Dadurch ergeben sich mehr Schwachstellen, die von Angreifenden genutzt werden können. Werden dementsprechend nicht ausreichend Schutzmechanismen etabliert und angewandt, steigt das Potenzial für Angriffe in der Automobilbranche.

## Welche Auswirkungen hatten die Vorfälle auf Ihr Unternehmen?

(Mehrfachauswahl möglich)



### Jedes dritte betroffene Unternehmen verzeichnet einen Schaden in Millionenhöhe

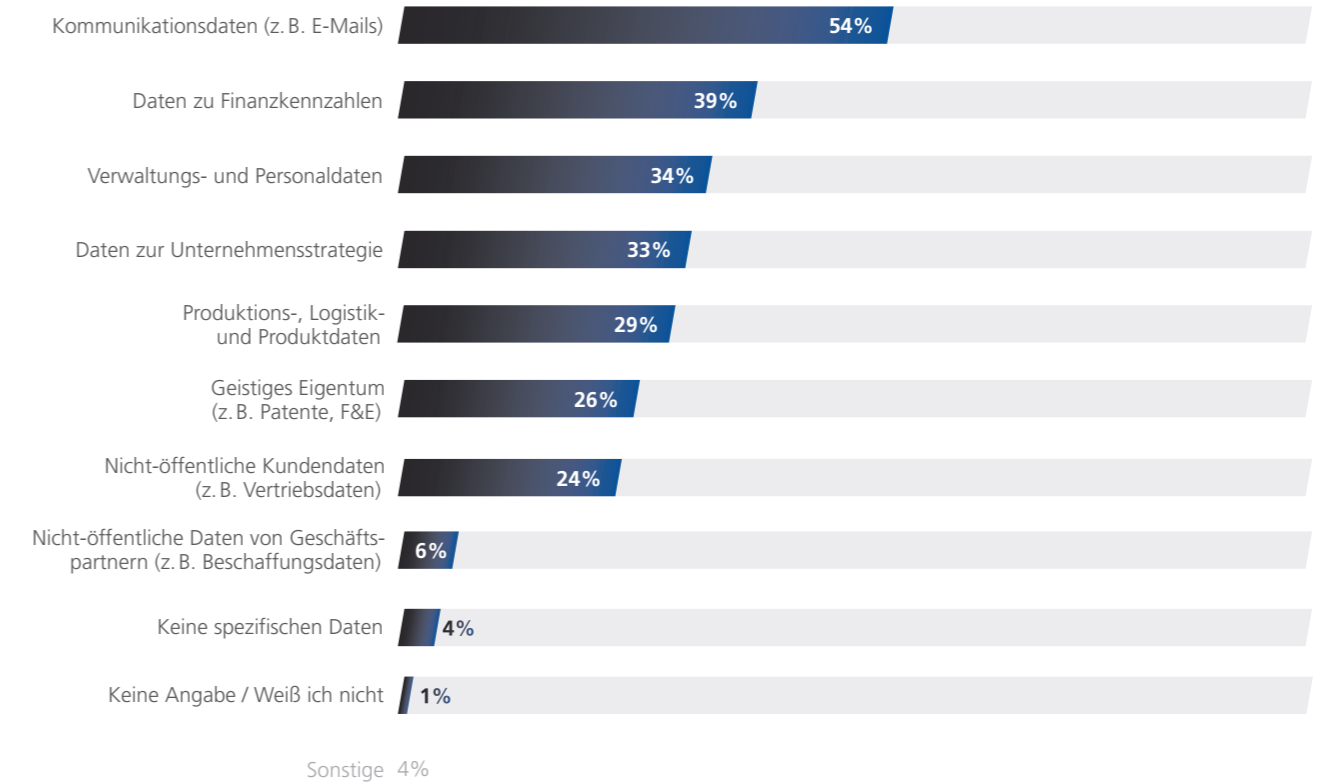
Über alle Unternehmensgrößen und Wirtschaftsbereiche hinweg erlitt ein Drittel der befragten Unternehmen durch einen erfolgten Angriff einen Schaden in Millionenhöhe. Von den kleinen Unternehmen, die Ziel eines Cyber-Angriffs wurden, geben 43 Prozent an, dass sich der aus dem Vorfall entstandene Schaden auf mindestens einhunderttausend Euro belief. Bei 47 Prozent der mittleren Unternehmen lag der Schaden bei fünfhunderttausend Euro und mehr. Jedes zweite (50 %) der großen Unternehmen verzeichnete einen Schaden von mindestens einer Million Euro. Mehr als ein Viertel (26 %) der Unternehmen mit mehr als 1.000 Mitarbeitenden verbuchte einen Schaden von mindestens fünf Millionen Euro, 6 Prozent sogar von mehr als zehn Millionen Euro.

Bei 40 Prozent aller Vorfälle, die einen Schaden nach sich zogen, handelte es sich um den Diebstahl von Betriebs-, Lieferanten- oder Kundendaten. Bei 38 Prozent der Angriffe wurden Systeme beschädigt oder Computer sabotiert. Und in knapp einem Drittel (32 %) der Fälle wurden Geschäfts- und Betriebsgeheimnisse verletzt.

Gefragt nach den drei Datenkategorien, die besonders schützenswert sind, gaben 48 Prozent der Teilnehmenden Verwaltungs- und Personaldaten an, 41 Prozent geistiges Eigentum, ebenfalls 41 Prozent Kommunikationsdaten (z. B. Kontaktdaten und Inhalte von E-Mails) und 35 Prozent Finanzkennzahlen. Große Unternehmen bewerten den Schutz von geistigem Eigentum (55 %) deutlich höher als mittlere (33 %) und kleine Unternehmen (27 %).

## Welche Daten waren im Rahmen Ihrer Vorfälle betroffen?

(Mehrfachauswahl möglich)



### Kommunikationsdaten sind bei der Hälfte der Vorfälle betroffen

Die Einschätzung dazu, welche Daten besonders schützenswert sind, deckt sich zu großen Teilen damit, welche Daten bei Cyber-Angriffen betroffen waren. So gaben 54 Prozent der Teilnehmenden von betroffenen Unternehmen an, dass bei Angriffen am häufigsten Kommunikationsdaten das Ziel waren, 39 Prozent nannten die unternehmensspezifischen Finanzkennzahlen und 34 Prozent die Verwaltungs- und Personaldaten. Auch, dass große Unternehmen ihr geistiges Eigentum als besonders schützenswert erachten, korrespondiert mit der tatsächlichen Lage. Bei 30 Prozent der großen Unternehmen war das geistige Eigentum Ziel eines Angriffs. Bemerkenswert ist, dass bei vielen Angriffen Daten zur Unternehmensstrategie betroffen waren, diese Datenkategorie bei den wichtigsten zu schützenden Datenkategorien aber erst an

sechster Stelle zu finden ist. Demnach bietet der Schutz der Daten zur Unternehmensstrategie einen Ansatzpunkt für Optimierungen. Unternehmen sollten ihren Fokus verstärkt hierauf legen. Ein ähnlicher Sachverhalt zeigt sich bei der Kategorie der Produktions-, Logistik- und Produktdaten. Diese sind bei knapp jedem dritten Angriff (29 %) Ziel, jedoch bei den schützenswerten Daten lediglich an siebter Stelle der Priorität in den Unternehmen. Die nicht öffentlichen Daten von Geschäftspartnern sind bei Vorfällen ein weniger betroffenes Angriffsziel. Bei kleinen Unternehmen waren hingegen speziell nicht öffentliche Kundendaten häufiger als bei mittleren oder großen Unternehmen im Rahmen eines Vorfalls betroffen.

## Welche Aspekte werden bei der Identifikation von IT-sicherheitsrelevanten Risiken berücksichtigt?

(Mehrfachauswahl möglich)



### Zentrale IT-Abteilung ist für die Identifikation von Cyber-Security-Risiken verantwortlich

Für die Identifikation von Cyber-Security-Risiken ist bei 64 Prozent der befragten Unternehmen die zentrale IT-Abteilung verantwortlich, bei 40 Prozent eine zuständige Fachabteilung für Informationssicherheit und bei 37 Prozent die Geschäftsführung beziehungsweise das C-Level-Management. Bei lediglich 2 Prozent der Unternehmen ist keine Instanz zuständig.

Bei den kleinen Unternehmen ist in 65 Prozent der Fälle die Geschäftsführung beziehungsweise das C-Level-Management für die Identifikation von Cyber-Security-Risiken verantwortlich. Das wirft die Frage auf, ob bei den involvierten Personen tatsächlich die notwendige Fachexpertise für diese Aufgabe vorliegt. Positiv ist allerdings, dass bei kleinen Unternehmen oftmals externe Dienstleister (35 %) hinzugezogen werden.

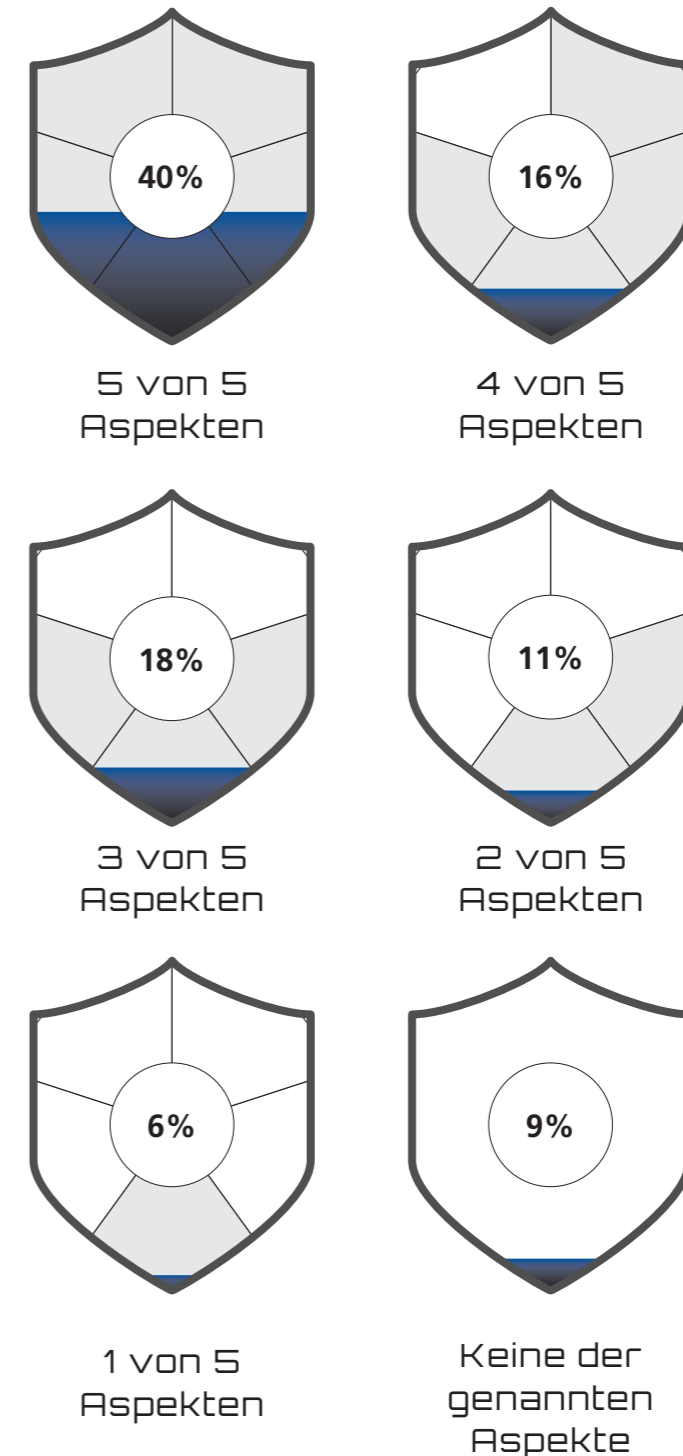
Insgesamt ist festzuhalten: Je größer das Unternehmen, desto häufiger liegt die Verantwortung bei der zentralen IT-Abteilung. Eine gesonderte Fachabteilung für die Identifikation von Cyber-Risiken ist bei 55 Prozent der großen Unternehmen etabliert.

### Vollumfängliche Risikobetrachtung findet in deutschen Unternehmen mehrheitlich keine Anwendung

85 Prozent der Teilnehmenden gaben an, bei der Identifikation von IT-sicherheitsrelevanten Risiken mögliche Angriffsziele zu berücksichtigen, 71 Prozent beschäftigten sich mit aktuellen Informationen über Bedrohungslagen, Angriffsstatistiken und Trends.

Tatsächlich geben lediglich 40 Prozent der Teilnehmenden an, alle der in obenstehender Abbildung dargestellten Aspekte bei der Analyse der IT-sicherheitsrelevanten Risiken im Blick zu haben. Das heißt im Umkehrschluss: Mehr als die Hälfte der deutschen Unternehmen hat keine umfassende Risikobetrachtung etabliert. 15 Prozent der Unternehmen beziehen keine der genannten Aspekte (9 %) oder lediglich einen Punkt (6 %) ein. Vor allem für diese Unternehmen besteht erhebliches Optimierungspotenzial.

## Verhältnis der in die Risikoidentifikation einbezogenen Aspekte



# EXPERTEN

# INTERVIEW

## Rudolf Näher Landeskriminalamt Baden-Württemberg

### Kurz Vita

**Rudolf Näher** ist seit 2016 beim LKA Baden-Württemberg als Referent für die Themenbereiche IT-Forensik und Datenanalyse tätig. Seit 2020 hat er die Leitung der zentralen Ansprechstelle Cybercrime inne.

### Kurzbeschreibung



Baden-Württemberg  
LANDESKRIMINALAMT

Das **Landeskriminalamt Baden-Württemberg** (LKA BW) ist die zentrale Dienststelle für besondere Aufgaben bei der Kriminalitätsbekämpfung in Baden-Württemberg. Das LKA BW sorgt als Zentralstelle für landeseinheitliche Standards, bietet zahlreiche Serviceleistungen für die Landespolizei und ermittelt in Fällen von besonderer Bedeutung. Die Zentrale Ansprechstelle Cybercrime (ZAC) ist als „Single Point of Contact“ für Wirtschaftsunternehmen, Behörden und öffentliche Stellen bei der Abteilung Cybercrime und Digitale Spuren angesiedelt. Dort sind Rudolf Näher und sein Team für die Bearbeitung sämtlicher Straftaten im Bereich Cybercrime zuständig. Fälle von Cybercrime aus dem Bereich der Wirtschaft und von öffentlichen Stellen werden bei der ZAC entgegengenommen, analysiert und bewertet. Außerdem werden polizeiliche Sofortmaßnahmen veranlasst. Gleichzeitig übernimmt die ZAC auch Präventionsaufgaben und gibt betroffenen Unternehmen Tipps und Informationen aus ihren bei anderen Ermittlungsverfahren gewonnenen polizeilichen Erkenntnissen. Neben der Durchführung von branchenspezifischen Cyber-Krisenübungen und Präventionsvorträgen werden beim Aufkommen neuer Modi Operandi oder dem Ausnutzen neuer Angriffsvektoren auch detaillierte Warnmeldungen erstellt und zielgerichtet veröffentlicht.

Das Gespräch zwischen Rudolf Näher (Landeskriminalamt Baden-Württemberg), Pascal Barreuther und Frank Cichon (beide MHP) wurde am 22. Juli 2021 per Videokonferenz geführt.

**Herr Näher, wenn wir den Unterschied zwischen Landeskriminalamt (LKA) und Bundeskriminalamt (BKA) im Thema Cyber Security beziehungsweise Cybercrime näher betrachten, wie würden Sie die Rollen der beiden Institutionen differenzieren?**

Für die Bekämpfung und Strafverfolgung von Cyber-Kriminalität sind grundsätzlich die Polizeibehörden der Bundesländer zuständig. Bei den Landeskriminalämtern (LKÄ) werden im Regelfall Pilot- und Mehrwertverfahren oder auch Verfahren geführt, die spezifisches Know-how oder auch spezielle technische Ausstattungen erfordern. Mittlerweile verfügen fast alle LKÄ über eine spezialisierte Abteilung Cybercrime. Seit 2012 steht darüber hinaus bei jedem LKA eine Zentrale Ansprechstelle Cybercrime als kompetenter Ansprechpartner für Wirtschaftsunternehmen zur Verfügung. Das BKA nimmt als Zentralstelle eher eine koordinierende Rolle ein, insbesondere, wenn starke Bezüge zu anderen Staaten bestehen. Es sammelt und stellt Informationen sowie Tools zur Verfügung, sodass effizient und zielgerichtet mit den vorhandenen polizeilichen Ressourcen umgegangen werden kann. Ermittlungen im Bereich Cybercrime werden dort nur im Rahmen der originären Zuständigkeit des BKA geführt. Etwa, wenn Einrichtungen des Bundes oder KRITIS (Kritische Infrastruktur)-Unternehmen betroffen sind. Hierzu wurde vor knapp eineinhalb Jahren eine Abteilung für Cybercrime beim BKA eingerichtet.

**Wie würden Sie die Bedeutung von Cyber Security in der heutigen Kriminalitätsbekämpfung beschreiben und hat sich diese durch die aktuelle Pandemie noch verändert?**

Wir unterscheiden zwischen Cybercrime im engeren Sinn und Cybercrime im weiteren Sinn. Cybercrime im engeren Sinn bezeichnet Straftaten, die sich zielgerichtet gegen IT-Systeme, IT-Infrastruktur und deren Daten richtet. Dazu zählen zum

Beispiel das Ausspähen sowie die Verschlüsselung von Daten oder gar die Sabotage der IT. In vielen Fällen ist eine klare Abgrenzung jedoch schwer und die Hintergründe der Tat vielfältig. Cybercrime im weiteren Sinn beinhaltet Fälle, in denen das Internet oder Informationstechnische Systeme als Tatmittel verwendet werden. Beispiele hierfür sind der Aufruf zu einer Straftat über das Internet oder auch Betrugsstraftaten, die über das Internet begangen werden. Betrachtet man nun den Verlauf der letzten Jahre, dann können wir sagen, dass Cybercrime in Gänze, das heißt sowohl im engeren als auch im weiteren Sinn, stark zugenommen hat. Ein kausaler Zusammenhang dieser Entwicklung mit der Corona-Pandemie lässt sich jedoch nur schwer ableiten. Mit zunehmender Vernetzung von immer mehr Geräten erhöhen sich auch die potenziellen Angriffsflächen für Cyber-Kriminelle. So ergeben sich beispielsweise durch von den Unternehmen während der Pandemie schnell ausgebaute Homeoffice-Lösungen weitere Angriffsvektoren wie schlecht oder unzureichend abgesicherte Fernzugänge, die von Cyber-Kriminellen ausgenutzt werden können. Auch DDoS-Attacken (Distributed Denial of Service), die sich bislang hauptsächlich gegen die Webpräsenzen von Unternehmen gerichtet haben, können nun gravierendere Auswirkungen haben, wenn plötzlich eine Vielzahl von Mitarbeitenden im Homeoffice nicht mehr auf die IT-Systeme des Unternehmens zugreifen kann und an der Arbeit gehindert wird.

**Wie würden Sie im Allgemeinen die Sensibilität bei deutschen Unternehmen oder bei der Wirtschaft in Bezug auf Cyber-Angriffe einschätzen?**

In den zurückliegenden Jahren kann man feststellen, dass ein Anstieg der Sensibilität stattgefunden hat und das Thema in deutschen Unternehmen zunehmend ernst genommen wird. Viele der Unternehmen nehmen mit uns Kontakt auf, wollen sich zum Beispiel gezielt auf Ransomware-Fälle vor-

bereiten und suchen den Schulterschluss zu Best Practices und Erfahrungswerten des LKAs. Weiterhin tragen IT-Sicherheitsgesetze, insbesondere in Bezug auf KRITIS-Unternehmen, dazu bei, dass diese mittlerweile sehr gut aufgestellt sind. Auf der anderen Seite gibt es weiterhin Weltkonzerne, die eklatante Lücken aufweisen. Hier ist womöglich oftmals die historisch gewachsene IT-Landschaft der Unternehmen ein Grund. Alte Maschinen oder sonstige Komponenten, die mit veralteten und nicht mehr unterstützten Betriebssystemen laufen und Sicherheitslücken aufweisen, aber aus finanziellen oder anderen Gründen noch in Betrieb sind. Oder auch ein unvollständiger Überblick über die im Verlauf der Zeit gewachsene, komplexe Infrastruktur und ein schlechtes Patch Management.

**Ist es Ihnen möglich, einen Vergleich hinsichtlich der Unternehmensgröße gemessen an der Mitarbeitendenzahl und der damit verbundenen Awareness zum Thema zu ziehen?**

In vielen Fällen, die bei uns zur Anzeige gebracht werden, sind insbesondere kleine Unternehmen hinsichtlich IT-Sicherheitskonzepten und Backup-Strategien schlecht aufgestellt. Exemplarisch können hier Unternehmen genannt werden, die vielleicht fünf oder sechs Clients betreiben und als zentralen Datenspeicher ein NAS nutzen. Dieses NAS wird von diesen Unternehmen oft fälschlicherweise als Back-up(-Ersatz) angesehen, mit entsprechenden Folgen im Fall einer Ransomware-Attacke oder auch in anderen Fällen, durch welche wichtige Daten unwiederbringlich verloren gehen. Diese Aspekte werden bei größeren Unternehmen schon umfassender und gründlicher betrachtet. Dennoch kann man hier nicht über alle Branchen hinweg pauschalisieren. Natürlich haben wir aber auch bei großen Unternehmen, die im Grunde sehr gut aufgestellt sind, Vorfälle. Eine hundertprozentige Sicherheit wird es nicht geben. Das zeigen insbesondere die jüngsten Supply-Chain-Angriffe, gegen welche man sich sehr schwer absichern kann, und

die auch große und sehr gut aufgestellte Unternehmen getroffen haben. Dennoch sollten sich Unternehmen bestmöglich gegen Cybercrime schützen, bevor es zu einem Angriff kommt.

**Für den Schutz sind die Bereiche Asset Management und Bedrohungsszenarien ein wichtiger Bestandteil. Welche Schwachstellen und Herausforderungen sehen Sie hier aktuell und was würden Sie als bedeutsamste Phänomene im Kontext von Cyber Security für die Unternehmen einschätzen?**

Das gefährlichste Phänomen sind Ransomware-Attacken, hier haben wir die häufigsten Fälle. Dies ist insbesondere auch auf ein verändertes Vorgehen der Täter\*innen in den vergangenen Jahren zurückzuführen. Waren es vor ein paar Jahren noch einzelne Akteure, sieht man inzwischen, dass die Angreifenden wie Unternehmen agieren. Es handelt sich dabei um organisierte Kriminalität, mit spezialisierten Entwicklern und einem professionelleren Modus Operandi. Anstatt wie früher E-Mails mit einem maliziösen Anhang zu verschicken, werden immer häufiger automatisiert Schwachstellen in ungepatchten Systemen ausgenutzt. Auch der gezielte Angriff auf Cloud-Anbieter oder IT-Dienstleister mit Fernzugriffen auf viele Unternehmen, um über diese eine Vielzahl von angeschlossenen Kunden anzugreifen, rückt vermehrt in den Fokus von Täter\*innen. Diese Akteure haben darüber hinaus festgestellt, dass viele Unternehmen mittlerweile, vielleicht auch aufgrund der medialen Präsenz von Ransomware-Attacken, eine funktionierende Back-up-Strategie besitzen. Daten werden deswegen von den Tätergruppierungen nicht mehr nur verschlüsselt, sondern zusätzlich auch ausgespäht. Die Drohung mit Veröffentlichung der ausgespähten Daten dient dann als weiteres Druckmittel. Auch eine Zunahme von Betrugsstraftaten wie Business-E-Mail-Compromise beziehungsweise das unbefugte Ändern von Bankverbindungen auf per E-Mail verschickten Rechnungen durch Abfangen

Wir unterscheiden zwischen Cybercrime im engeren Sinne und Cybercrime im weiteren Sinne:

## Cybercrime im engeren Sinne

bezeichnet Straftaten, die sich zielgerichtet gegen IT-Systeme, IT-Infrastruktur und deren Daten richtet. Dazu zählen zum Beispiel das Ausspähen sowie die Verschlüsselung von Daten oder gar die Sabotage der IT. In vielen Fällen ist eine klare Abgrenzung jedoch schwer und die Hintergründe der Tat vielfältig.

## Cybercrime im weiteren Sinne

beinhaltet Fälle, in denen das Internet oder Informationstechnische Systeme als Tatmittel verwendet werden.

Beispiele hierfür sind der Aufruf zu einer Straftat über das Internet oder auch Betrugsstraftaten, die über das Internet begangen werden.

**Rudolf Näher**

Leiter der Zentralen Ansprechstelle Cybercrime (ZAC)  
Landeskriminalamt Baden-Württemberg

der Kommunikation hat zuletzt zugenommen und führt zu hohen monetären Schäden. Trotz dieser Entwicklung der Kriminalität sehe ich hauptsächlich fehlende oder mangelhafte Back-up-Strategien, eine mangelhafte Absicherung von Konten (bspw. mittels Multi-Faktor-Authentifizierung) sowie ein schlechtes Patch Management als gravierendste Risiken beim Schutz von Daten an. Es ist ganz einfach, gezielt nach IT-Systemen mit bestimmten Betriebssystemen und angreifbaren Softwareständen über Suchmaschinen zu suchen und anschließend automatisiert zu attackieren. Es geht vor allem um die kontinuierliche Aktualisierung der Systeme. Sobald Updates beziehungsweise Patches verfügbar sind, sollten diese auch zeitnah durchgeführt werden, da Sicherheitslücken in immer kürzerer Zeit nach Bekanntwerden durch Cyberkriminelle ausgenutzt werden.

**Sie haben erwähnt, dass viele Unternehmen keine ausgearbeitete Back-up-Strategie haben und diese dementsprechend auch nicht getestet wurde. Haben Sie schon die Erfahrung gemacht, dass sich Unternehmen nach einem Angriff und Ihren Ermittlungen stärker mit dem Thema befassen?**

Polizeiliche Ermittlungen bieten auch den betroffenen Unternehmen einen Mehrwert, auch wenn wir beispielsweise verschlüsselte Daten nicht entschlüsseln oder die IT-Systeme wieder aufbauen. Die polizeilichen Erfahrungswerte nützen insoweit, als dass wir durch eigene forensische Analysen meist Täter\*innen und Vorgehen kennen und diese Informationen zur Verfügung stellen können. Also zum Beispiel: Wie sind die Täter\*innen eingedrungen? Was waren die ausgenutzten Angriffsvektoren? Wie wurde agiert? Welche Systeme waren betroffen? Und wie lange waren die Täter\*innen schon auf diesen tätig? Dies dient dem Unternehmen für den Wiederaufbau der IT-Systeme und bewahrt so vor der falschen Herangehensweise bei der Wiederherstellung der Daten aus dem Back-up. Oftmals ist es dann auch der Fall, dass betroffene

Unternehmen nach dem Angriff und den Erkenntnissen daraus ihre IT gänzlich neu und gehärtet aufsetzen. Dies ist meist jedoch kostenintensiver, als sich vorab präventiv um IT-Sicherheitsmaßnahmen zu kümmern.

**Strategien auf dem neusten Stand zu haben, ist ebenso wichtig wie die Daten selbst. Welche Elemente sollte eine Back-up-Strategie auf jeden Fall beinhalten?**

Grundsätzlich sollte man mehrere Back-ups auf unterschiedlichen Medien vorhalten. Außerdem sollte mindestens eines dieser Back-ups physisch vom restlichen Netz getrennt sein. Idealerweise findet die Lagerung sogar an einem anderen Ort statt. Insbesondere, wenn man im Rahmen einer ganzheitlichen Betrachtung neben den Gefahren aus dem Cyber-Bereich auch physische Gefahren für die Daten im Blick hat – wie ein Feuer oder Wasserschäden. Sollte das physisch getrennte Back-up in solchen Fällen am gleichen Ort sein, ist auch in solch einem Fall ein Verlust der Daten unumgänglich.

**Betrachten wir noch einmal den Bereich Supply Chain. Können Sie sagen, ob für Unternehmen das Schadenspotenzial zukünftiger Bedrohungsszenarien größer wird?**

Ich glaube, insbesondere Supply-Chain-Attacken müssen zukünftig mehr im Blick gehalten werden. Man muss hier berücksichtigen, dass jeder Einsatz von externen Softwareprodukten oder IT-Dienstleistern und Zulieferern mit Verbindungen auf die eigenen IT-Systeme trotz Einhaltung von IT-Sicherheitsstandards ein gewisses Risiko birgt. Für Angreifende ist es lukrativ und effizient, wenn ein Produkt oder ein Unternehmen angegriffen wird und aufgrund der Verbindungen zu deren Kunden dann beispielhaft mehrere Tausend weitere Unternehmen angreifbar sind.

### Welche grundsätzliche Frage sollte sich ein Unternehmen hinsichtlich der jeweiligen schützenswerten Güter stellen?

Die grundsätzliche Überlegung sollte sein, wie lange das jeweilige Unternehmen in welchen Bereichen ohne die IT überlebensfähig wäre. Darauf aufbauend müssen Risiken abgeschätzt und die wichtigsten IT-Systeme und Anwendungen identifiziert werden, die für den Betrieb absolut notwendig sind. Fragen, die gestellt werden müssen, sind beispielsweise: Wie wichtig sind die Daten? Wie wichtig sind die IT-Systeme an sich und für das Erbringen meiner Leistung? Schließlich muss eine umfassende Risikobewertung vorgenommen, darauf aufbauend müssen Sicherheitsmaßnahmen umgesetzt werden.

### Präventive Maßnahmen können Unternehmen vor Schäden schützen. Was würden Sie als grundsätzliche Maßnahmen sehen, die Unternehmen treffen oder etablieren sollten, um einen tatsächlichen Angriff mit möglichst geringem Schaden zu überstehen?

Ganz wichtig ist, dass man eine umfassende Risikobewertung vornimmt, entsprechende Maßnahmen umsetzt und sich außerdem gedanklich auf Cyber-Angriffe und IT-Sicherheitsvorfälle vorbereitet – und darauf aufbauend entsprechende Notfallpläne für den Worst Case erstellt. Ganz wichtig ist hierbei auch, dass man diverse Szenarien wirklich auch Schritt für Schritt durchspielt und übt. Nur durch Üben können oftmals Kleinigkeiten entdeckt werden, die zuvor nicht bedacht wurden, aber im Ernstfall gravierende Auswirkungen haben können. Es gab beispielsweise schon Fälle, in denen zwar ein Back-up-Konzept bestand, das Back-up jedoch über Monate fehlerhaft erstellt wurde, ohne dass dies bemerkt wurde, und somit im Ernstfall nicht zu gebrauchen war. Auch die Kommunikation und die (physische) Zugänglichkeit von Notfallplänen im Fall von Verschlüsselungen sollte man hierbei im Blick haben. Darüber hinaus ist es sehr wichtig,

dass nicht nur auf technische Maßnahmen eingegangen wird, sondern auch organisatorische Maßnahmen vorbereitet werden. Beispielsweise ein Notfallplan, in dem klare Rollen und Entscheidungsbefugnisse definiert sind, um im Ernstfall schnelle Entscheidungen treffen zu können. Letztendlich sollten in jedem Unternehmen umfassende und aktuelle Netzwerkpläne vorhanden sein. Insbesondere zur Eingrenzung des Angriffs und bei der Einbindung von Dritten zur Schadensbewältigung sind diese Pläne essentiell für effiziente Incident-Response-Maßnahmen. Darüber hinaus stellen die Netzpläne auch eine unverzichtbare Basis für grundlegende IT-Sicherheitsmaßnahmen und das Patch Management dar.

### Um effizient auf Angriffe reagieren zu können, nutzen Unternehmen als Teil ihres Managementsystems vermehrt Notfall- oder Reaktionspläne. Welchen Mehrwert bietet es Ihrer Meinung nach, ein solches Managementsystem zu etablieren?

Grundsätzlich bereitet man sich schon mal gedanklich auf mögliche Fälle vor. Außerdem beobachten wir immer wieder, dass IT-Sicherheitsvorfälle effizienter bewältigt werden, wenn man sich gut auf solche Fälle vorbereitet. Wenn es so etwas nicht gibt, dann herrscht oftmals aufgrund mangelnder Verantwortlichkeit und fehlender Organisation Chaos. Dadurch geht den Unternehmen oft wichtige Zeit verloren. Zum einen aus unternehmerischer Sicht, um die IT-Systeme wieder aufzusetzen und den Betrieb schnellstmöglich wieder zum Laufen zu bekommen. Aber auch aus polizeilicher Sicht ist es für uns wichtig, Teil eines Notfallplanes zu sein und frühzeitig eingebunden zu werden, da wir oftmals wichtige Spuren hätten sichern können, die durch falsche Herangehensweise oder bedingt durch den Zeitverzug bis zur Meldung bei uns verloren gehen.

### Polizeiliche Ermittlungen werden als eine reaktive Maßnahme zur Bewältigung von Cybercrime gesehen. Inwiefern glauben Sie, dass

### Unternehmen Angst vor der öffentlichen Bekanntgabe haben und mit Folgeangriffen oder einem Reputationsschaden rechnen, sobald die Polizei involviert wird?

Unternehmen machen sich Gedanken um Reputationsschäden. Wobei das eher unbegründet ist. Wir als Polizei dürfen keine Information nach draußen geben. Oftmals besteht auch die Annahme, dass die Polizei sowieso nicht helfen kann, sondern eher behindert. Dabei sprechen wir jede unserer Maßnahmen eng mit dem betroffenen Unternehmen und gegebenenfalls hinzugezogenen externen Dienstleistern ab und haben zu jeder Zeit die Interessen des angegriffenen Unternehmens im Blick. Die größten Vorteile polizeilicher Ermittlungen sind darüber hinaus oft erst später ersichtlich. Auch wenn wir in einem konkreten Fall einem betroffenen Unternehmen nicht direkt helfen können, so können wir aufgrund exklusiver rechtlicher Befugnisse und technischer Mittel oftmals viele andere Unternehmen, die bereits im Visier der gleichen Angreifenden sind, vor einer unmittelbar bevorstehenden Attacke warnen.

### Die aktuelle Entwicklung lässt darauf schließen, dass Cybercrime auch in Zukunft eine immer wichtigere Rolle spielen wird. Wie würden Sie das LKA zukünftig als Partner in diesem Bereich platzieren wollen und worauf sollten Unternehmen besonders achten?

Wir hoffen natürlich, dass Unternehmen noch öfter den Kontakt zu uns suchen und keine Angst vor einem Reputationsverlust oder einer Behinderung des Wiederaufbaus der IT-Systeme haben. Wir gehen von Amts wegen verschwiegen vor, haben immer die Interessen des geschädigten Unternehmens im Blick und kommen auch nicht im Streifenwagen, sondern ganz unauffällig und wenn notwendig auch unter einer Legende. Je öfter wir gerufen werden, desto häufiger haben wir die Chance, Spuren zu sammeln, zusammenzuführen

und beispielsweise mit Telekommunikationsüberwachungsmaßnahmen Täterinfrastrukturen zu überwachen. So können wir gerichtsfeste Erkenntnisse über die Täter\*innen erlangen, weitere Unternehmen vor Schaden bewahren und eine Verschlüsselung der Daten von weiteren potenziellen Opfern verhindern. Im Endeffekt machen wir so auch das „Geschäftsmodell“ der Täter\*innen weniger lukrativ. Zusätzlich möchten wir unsere Kooperationen mit Wirtschaftsunternehmen und -verbänden vorantreiben. Da die Modi Operandi und die Techniken sich ständig weiterentwickeln, möchten wir uns mehr mit der Wirtschaft verzahnen, effizienter agieren und so Wissen über weitere Strecken teilen. Ein gemeinsames Verständnis von der Bedrohungslage und eine enge und kooperative Zusammenarbeit, auch im Fall eines Cyber-Angriffs, bieten Vorteile für alle Beteiligten. Worauf Unternehmen in Zukunft achten sollten, ist meiner Meinung nach der Anstieg von Supply-Chain-Attacken. Wenn externe Zulieferer und IT-Dienstleister engagiert werden, die Zugriff auf die IT haben, sollten sich Unternehmen vertraglich absichern und es sollte eine kontinuierliche Prüfung durchgeführt werden, sodass festgelegte IT-Sicherheitsstandards, -konzepte und -maßnahmen auch umgesetzt und eingehalten werden. Durch den weiteren Anstieg an Vernetzung von Endgeräten mit dem Internet werden zukünftig auch mehr Angriffsvektoren geschaffen. DDoS-Attacken könnten in Zukunft in Kombination mit anderen Phänomenen auch ein weiteres spannendes Thema sein. Abschließend sollte alles rund um Ransomware-Gruppierungen nicht außer Acht gelassen werden, wobei hier zukünftig eventuell auch vermehrt Innentäter\*innen, die Informationen über Sicherheitslücken oder Ähnliches gegen eine Provision an Ransomware-Gruppierungen weitergeben, eine Rolle spielen können.

### Herr Näher, wir danken Ihnen ganz herzlich für Ihre spannenden Einblicke und das interessante Gespräch.



„Ganz wichtig ist, dass man ein Gefahrenbewusstsein hat und eine umfassende Risikobewertung vornimmt, entsprechende Maßnahmen umsetzt und sich außerdem gedanklich auf Cyber-Angriffe und IT-Sicherheitsvorfälle vorbereitet.“

Das Credo muss lauten: Keine Digitalisierung ohne Cyber Security. Und dazu kommt immer auch die umfassende Incident-Response-Planung für den Fall der Fälle.“

**Andreas Stenger**

Präsident Landeskriminalamt Baden-Württemberg



## 2.2 Reaktive Vorfallsbehandlung

### Genutzte Schwachstellen variieren nach Unternehmensgröße

Von den Unternehmen, die schon einmal von einem IT-sicherheitsrelevanten Vorfall betroffen waren, wurden die Konfiguration von Systemen (39%), die jeweiligen Betriebssysteme von Geräten (32%) sowie die Fremd- und Privatgeräte (31%) am häufigsten als Schwachstellen genannt. Hinsichtlich der Betriebssysteme ist wichtig, dass diese nicht nur auf Servern, Rechnern oder Smartphones laufen, sondern beispielsweise auch auf Geräten wie Kopierern. Die Systemlandschaft, die Schwachstellen aufweist, ist also stark ausdifferenziert.

Vom Gesamtbild über alle Unternehmensgrößen hinweg weichen die Angaben der Teilnehmenden aus kleinen Unternehmen merklich ab. Sie nannten mit jeweils 57 Prozent die Fremd- und Privatgeräte sowie die Mitarbeitenden am häufigsten als Schwachstellen. Auf Rang drei folgen mit 43 Prozent die Softwareanwendungen – beispielsweise Webbrowsern oder E-Mails. Dass zwei Schwachstellen auf den ersten beiden Plätzen liegen, die einen unmittelbaren Bezug zum Verhalten der Nutzenden aufweisen, lässt möglicherweise auf eine geringere

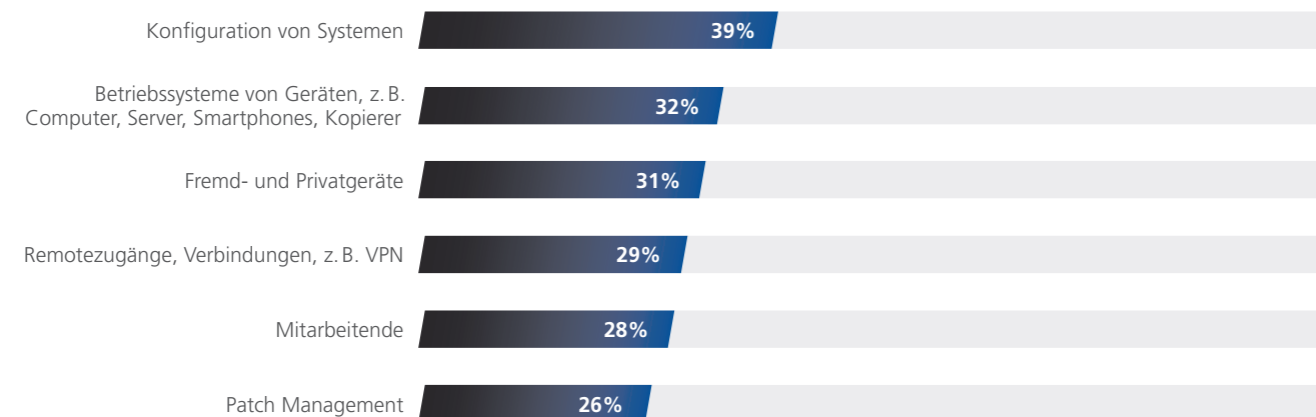
Kapazität für Schulungsmaßnahmen und damit zusammenhängend auf eine mangelnde Aufmerksamkeit für Bedrohungen schließen.

Bei den mittleren Unternehmen entspricht die Einschätzung weitgehend dem Gesamtbild: Betriebssysteme wurden von 33 Prozent der Teilnehmenden als Schwachstellen identifiziert, die Konfiguration von Systemen und die Softwareanwendungen jeweils von 32 Prozent. Ähnlich sieht es bei den großen Unternehmen aus. Mit 48 Prozent wird hier die Konfiguration der Systeme am häufigsten als Schwachstelle angegeben, gefolgt von Remote-Zugängen (35%) und den Betriebssystemen von Geräten (33%).

Dass Remote-Zugänge vor allem von den großen Unternehmen sehr häufig genannt wurden, könnte auf die Corona-Pandemie und die damit verbundene rasante Zunahme des Homeoffice-Anteils zurückzuführen sein. Aus Sicht der IT-Sicherheit ist auf diese Entwicklung besonderes Augenmerk zu legen. Entscheidend wird sein, einen besseren Schutz der Remote-Zugänge zu etablieren und das von dieser Schwachstelle ausgehende Risiko signifikant zu mitigieren.

### An welchem Punkt trat die Schwachstelle auf?

(Auswahl der häufigsten Antworten / Mehrfachauswahl möglich)



Unter **reaktiver Vorfallsbehandlung** werden die für ein Unternehmen relevanten Prozesse und Tätigkeiten verstanden, mit denen schnellstmöglich auf die Auswirkung eines informationssicherheitsrelevanten Vorfalls reagiert wird.

**Ziel** ist es, die **Betriebsfähigkeit aufrechtzuhalten**, Sicherheitslücken zu schließen sowie den Betrieb wiederherzustellen.

„Die größten Vorteile polizeilicher Ermittlungen sind darüber hinaus oft erst später ersichtlich. Auch wenn wir in einem konkreten Fall einem betroffenen Unternehmen nicht direkt helfen können, so können wir aufgrund exklusiver rechtlicher Befugnisse und technischer Mittel oftmals viele andere Unternehmen, die bereits im Visier der gleichen Angreifenden sind, vor einer unmittelbar bevorstehenden Attacke warnen.“

**Rudolf Näher**

Leiter der Zentralen Ansprechstelle Cybercrime (ZAC)  
Landeskriminalamt Baden-Württemberg

**Phishing und Hacking als präferierte Angriffsarten**

Zu den Angriffsarten, die am häufigsten Schäden verursacht haben, gehören Phishing (54 %), Hacking (54 %), Ransomware (45 %) und Spyware (33 %). Social Engineering wurde bei jedem dritten Angriff (29 %) als Werkzeug genutzt. Die Ergebnisse des Reports zeigen auf, dass ein Cyber-Angriff überwiegend aus einer Kombination verschiedener Angriffsarten besteht. Infolge ist zu erwarten, dass deutsche Unternehmen auch zukünftig oftmals Kombinationen aus beispielsweise Phishing, Hacking und dem Einsatz von Ransomware gegenüberstehen. Da solche Angriffe eine besondere Herausforderung sind, ist unserer Erfahrung nach ein breites Schulungsangebot sowie ein vielseitiges Monitoring erforderlich.

**Umfeld der Angreifenden ist mehrheitlich bekannt**

Ein Cyber-Angriff lässt sich überdurchschnittlich häufig auf ein spezifisches Umfeld zurückführen: 59 Prozent der Teilnehmenden gaben an, dass Hacker\*innen für den Angriff verantwortlich waren, 31 Prozent nannten Hacktivist\*innen und jeweils 30 Prozent identifizierten Geschäftspartner und Wettbewerber als Angreifende. Lediglich vier Prozent der befragten Unternehmen konnten keine Angaben zum Umfeld der Angreifenden tätigen.

**Hälfte der Unternehmen informiert die Polizei**

Von mehr als zwei Dritteln (76 %) der Unternehmen werden die Mitarbeitenden über einen IT-sicherheitsrelevanten Vorfall informiert. Die Aufsichtsbehörde wird in 64 Prozent der Vorfälle benachrichtigt. Dass eine Meldung an die Aufsichtsbehörden erfolgt, hängt auch mit den gesetzlichen Vorgaben der DSGVO und damit verbundenen Meldepflichten zusammen.

Auffällig ist, dass die Häufigkeit der Einbindung der Aufsichtsbehörde mit der Größe des Unternehmens steigt. So melden nur 37 Prozent der kleinen Unternehmen einen Vorfall der Aufsichtsbehörde (11 Prozent machten keine

Angabe oder wissen es nicht). Bei den mittleren Unternehmen melden 64 Prozent, bei den großen Unternehmen 75 Prozent einen Vorfall einer Aufsichtsbehörde.

Die verantwortliche Polizeibehörde, beispielsweise das jeweilige LKA, wird bei einem IT-sicherheitsrelevanten Vorfall von 53 Prozent der befragten Unternehmen informiert. Jeder Vorfall, der einer Polizeibehörde bekannt und von ihr untersucht wird, trägt dazu bei, potenzielle Angreifende und Angriffsmuster zu identifizieren und ermöglicht so, andere Unternehmen zu warnen.

**Hälfte der Unternehmen nimmt externe Unterstützung bei der Vorfallsbewältigung in Anspruch**

Bei der Aufarbeitung von IT-sicherheitsrelevanten Vorfällen wird von mehr als der Hälfte aller Unternehmen eine externe Beratung (56 %), eine Polizeibehörde (54 %) oder eine Aufsichtsbehörde (53 %) einbezogen. 46 Prozent der Teilnehmenden gaben an, eine Versicherung einzubeziehen, 44 Prozent nannten das Bundesamt für Sicherheit in der Informationstechnik (BSI).

77 Prozent der Unternehmen, die eine Polizeibehörde bei einem Vorfall informieren, binden diese ebenfalls in die weitere Behandlung des Vorfalls ein. 63 Prozent der befragten Unternehmen gaben an, sie würden auch dann die Polizei in die Bewältigung des Vorfalls einbinden, wenn bereits eine Versicherung informiert wurde. Wie in unserem Experteninterview mit Rudolf Näher (LKA Baden-Württemberg) herausgearbeitet wurde, kann durch die Ermittlungen seitens einer Polizeibehörde oftmals von einem einzelnen Vorfall auf eine Vielzahl weiterer potenzieller Angriffe rückgeschlossen werden. Die Einbindung führt somit zur Benachrichtigung anderer Unternehmen. Jedes Unternehmen, das die Polizeibehörde einbindet, hilft dabei, weitere Unternehmen zu schützen und Schäden durch Cyber-Angriffe in Deutschland zu mitigieren. Insofern ist es wichtig, die Polizeibehörden einzubeziehen, auch wenn beispielsweise eine Versicherung bereits informiert wurde.

### Durch welche Angriffsarten wurden Schäden verursacht?

(Mehrfachauswahl möglich)

**54%**

**Phishing und Hacking**  
 (z. B. Täuschung durch vertrauenswürdige E-Mails oder Webseiten) (z. B. Ausnutzung von Schwachstellen)

**45%**

**Ransomware**  
 (z. B. Verschlüsselung von Unternehmensdaten)

**33%**

**Spyware**  
 (z. B. Ausspähung von Nutzeraktivitäten oder sonstige Daten)

**29%**

**Social Engineering**  
 (Beeinflussung von Personen, um beispielsweise vertrauliche Informationen preiszugeben oder Sicherheitsfunktionen auszuhebeln)

**25%**

**Denial of Service**  
 (z. B. Überlastung von Web- oder E-Mail-Servern)

**13%**

**Sonstige Malware**  
 (z. B. Viren, Bots, Würmer oder Trojaner)

**3%**

**Keine Angabe / Weiß ich nicht**

**1%**

**Sonstige**

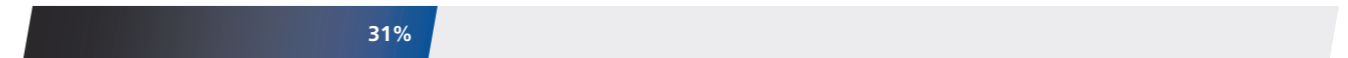
### Welchem Umfeld lassen sich die Angreifenden der Vorfälle zuordnen?

(Mehrfachauswahl möglich)

**59%**

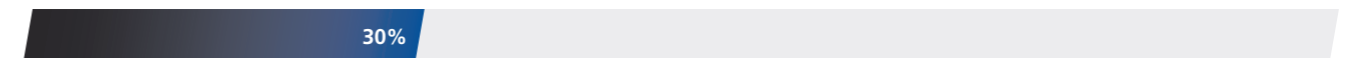
**Kriminelle Hacker\*innen**

(Personen, die Lücken in fremden Systemen unerlaubt für eigene, oft kriminelle Zwecke wie den Diebstahl von Informationen nutzen)

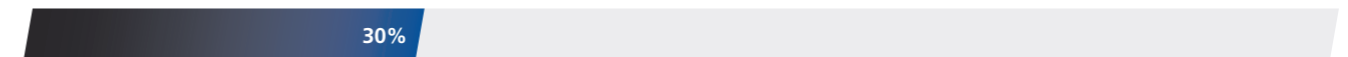


**Hacktivist\*innen**

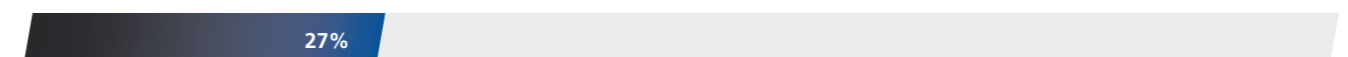
(Person, die sich unbefugten Zugriff auf Computerdateien oder Netzwerke verschafft, um soziale oder politische Ziele zu verfolgen)



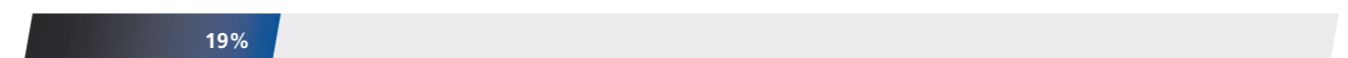
**Geschäftspartner\*innen**



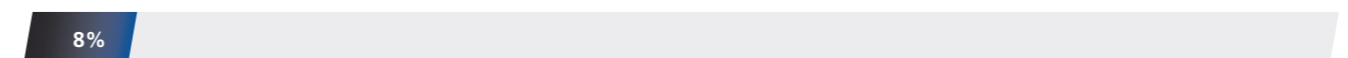
**Wettbewerber**



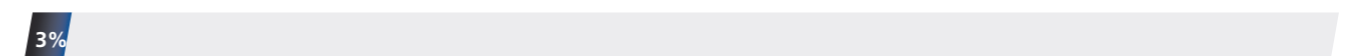
**Staatliche Nachrichtendienste und Akteure**



**Ehemalige Mitarbeitende**



**Aktive Mitarbeitende (Innentäter\*innen)**



**Keine Angabe / Weiß ich nicht**

# EXPERTEN

# INTERVIEW

## Bernd Bauer Siemens AG

### Kurz Vita

Bernd Bauer ist seit 1998 bei der Siemens AG in verschiedenen Positionen beschäftigt. Im Jahr 2018 wurde er Teil der Cyber-Security-Organisation bei Siemens und verantwortet heute innerhalb der CYS die Einheit Protection und Consulting Services (PCS). In seiner Rolle als Head of PCS leitet er unter anderem Projekte, die den allgemeinen Reifegrad der Cyber-Sicherheit bei Siemens weltweit verbessern. Dabei stehen der Schutz von IT/OT-Infrastruktur, die Sicherung von Produkten, Dienstleistungen und Lösungen sowie die Unterstützung der Siemens-Geschäftsbereiche bei der Schaffung eines hochwertigen Cyber-Security-Angebotes im Fokus. Zuvor war Bernd Bauer langjährig als Partner IT Audit und Digitalization Officer für die IT Revision inklusive der IT-Sicherheit bei Siemens zuständig.

### Kurzbeschreibung Siemens CYS/CSIP

## SIEMENS

Cyber Security ist ein kritischer Erfolgsfaktor für Unternehmen. Deshalb hat Siemens beschlossen, seinen Schutz zu verbessern und dadurch zu einem führenden Unternehmen in Sachen IT-, OT- sowie Produkt- und Lösungssicherheit zu werden. Auf Basis eines Benchmarks und der Ergebnisse interner Audits wurden verschiedene Verbesserungsbereiche identifiziert und Ziele für ein neues Cybersecurity Improvement Program (CSIP) definiert. Seit des Kick-offs des Lenkungsausschusses im April 2018 wurden viele Projekte abgeschlossen und die Leistungen/Ergebnisse an die Linienorganisation übergeben. Zum Ende des Fiskaljahres 2021 wurde das CSIP erfolgreich abgeschlossen.

Das Gespräch zwischen Bernd Bauer (Siemens), Andreas Henkel und Michael Schmitt (beide MHP) wurde am 13. August 2021 per Videokonferenz geführt.

### Als Head of Protection and Consulting Services im Bereich Cyber Security unterstützen Sie aktiv die Siemens AG weltweit bei der Gewährleistung der IT-Sicherheit. Welche Bedeutung hat Cyber Security Ihrer Meinung nach in der verarbeitenden Industrie?

Cyber Security nimmt einen immer größer werdenden Stellenwert ein. Mit steigendem Digitalisierungsgrad, zunehmender Vernetzung und größerer Cloudifizierung der Unternehmen in der verarbeitenden Industrie multiplizieren sich die Angriffsvektoren für mögliche Cyber-Attacks.

### Wie ist in diesem Kontext der Stellenwert von Cyber Security bei Siemens einzuordnen?

Der Stellenwert hat sich über die vergangenen Jahre sehr stark verändert. Früher war Cyber Security eine Funktion, die mehrere Ebenen unter dem Management Board angesiedelt war und in unterschiedliche Verantwortlichkeiten wie Product Service Solutions, Infrastruktur oder auch Business Managed IT untergliedert wurde. Mit der Gründung der Cyber-Security-Organisation im Jahr 2018 wurde die Verantwortung für Cyber Security zentralisiert und ein holistischer Ansatz mit IT-, OT- und Produktsicherheit gewählt. Durch die direkte Berichterstattung an den Vorstand der Siemens AG wurde dem Thema Cyber Security ein neuer Stellenwert gegeben und die zentrale Bedeutung unterstrichen.

### Aus welchem Grund hat man sich bei Siemens mit dem Thema Cyber-Sicherheit so positioniert?

Ein zentraler Bestandteil der Siemens-Strategie ist die Digitalisierung des Unternehmens. Um eine erfolgreiche digitale Transformation zu ermöglichen, muss die Cyber Security ein elementarer Bestandteil des Rahmenwerks sein. Digitale

Plattformen oder auch die Automatisierung in den Werken sind abhängig davon, Risiken und mögliche Angriffsvektoren zu kennen und zu minimieren, um den bestmöglichen Schutz unserer Daten und Assets zu ermöglichen. Als Beispiel kann man hier den Fall Stuxnet nennen. Hierbei wurden vor circa zehn Jahren Zentrifugen für die Uran-Aufbereitung im Iran als Ziel eines Cyber-Angriffs zerstört. Die Steuerung dieser Anlagen basierten auf Siemens S7 (Basissoftwarepaket zur Programmierung und Konfiguration von Automatisierungssystemen). Wir haben im Zuge dieses Events gelernt, dass schon in der Produktentwicklung Sicherheitsmaßnahmen als Security by Design von Anfang an berücksichtigt werden müssen. Für Siemens als renommiertem Digitalisierungs- und Automatisierungspartner ist es unerlässlich, Cyber Security in seinem digitalen Offering zu inkludieren und ebenfalls unsere Kunden zu schützen.

### Die Risiken von Cyber-Angriffen haben sich in den letzten Jahren massiv gewandelt. Welche Bedrohungsszenarien haben sich als die größten Gefahren herausgestellt und was macht Siemens mit den gewonnenen Erkenntnissen, um zukünftige Angriffe zu verhindern?

Eine der größten Bedrohungen ist Ransomware. Im Fall eines Major Incidents bei Siemens wird eine Root Cause Analysis durchgeführt, um den Ursprung der Cyber-Attacke und den Angriffsvektor, der zum Erfolg geführt hat, zu ermitteln. Um solche Events in Zukunft zu verhindern, ist es notwendig, seine Assets zu kennen und ein Asset Management aufzubauen. Nur wenn ich meine Asset-spezifischen Risiken identifiziert und bewertet habe, können entsprechende präventive und auch reaktive Maßnahmen etabliert werden. Somit können auch bei dem Eintritt eines IT-sicherheitsrelevanten Vorfalls unmittelbar Gegenmaßnahmen eingeleitet werden. Im Kontext eines ganzheitlichen Asset Managements werden Detection Agents installiert, um Angriffe zu iden-

tifizieren, und in Verbindung mit der Incident Response der eigenen Systemplattform werden diese Attacks eingegrenzt, Ziele abgeschirmt sowie Angreifende abgewehrt und Daten und Systeme wiederhergestellt. Diese Herangehensweise wird als kontinuierlicher Prozess durchgeführt, um aus der Root Cause Analysis von Angriffen Maßnahmen abzuleiten. Wir haben dieses Vorgehen ebenfalls im Rahmen des CSIP durchgeführt, um eine strukturierte Abarbeitung von identifizierten Root Causes zu ermöglichen.

### Können Sie uns ein Beispiel nennen, wie Sie auf Basis der Root Cause Analysis geeignete Maßnahmen identifiziert haben?

Hierzu können wir das Thema laterale Bewegungen im Netzwerk einmal betrachten. Um hierzu entsprechende Maßnahmen abzuleiten, müssen im ersten Schritt beispielsweise laterale Bewegungen im Netzwerk identifiziert werden. Denn bei diesen lateralen Bewegungen werden zuerst Credentials gestohlen, um sich im schlechtesten Fall damit durch das gesamte Unternehmensnetzwerk durchzumanövrieren und entsprechende Ziele im Netzwerk anzugreifen. Um das Risiko dieses Angriffsvektors zu minimieren, wurden bei Siemens unterschiedliche Maßnahmen definiert. Dazu gehören unter anderem eine angepasste Password Policy, um einfache beziehungsweise leicht zu erratende Passwörter zu vermeiden; die Einführung von Detection Agents auf allen End Points und Servern sowie der Aufbau eines Privileged Access Managements. Außerdem wurde die Reduktion der lokalen Admin-Rechte veranlasst und durchgeführt. Denn ohne lokale Admin-Rechte können keine Programme, wie beispielsweise Malware, mehr ausgeführt werden.

### Mit welchen Cyber-Security-Herausforderungen haben Sie aktuell im täglichen Geschäft zu kämpfen?

Eine der größten Herausforderungen ist die Bereitstellung notwendiger Mittel wie Finanzierung und Ressourcen. Im täglichen Geschäft stehen Produktivität und Kosten im Vordergrund. Da Cyber Security nicht mittelbar zu einem zusätzlichen Revenue führt, ist es umso wichtiger, die Bedeutung der Risikominimierung durch Cyber Security hervorzuheben. Wir gehen bei Siemens Cyber Security proaktiv an – und nicht nur reaktiv und aus einer Risikosicht. So lassen sich auch Chancen und Wettbewerbsvorteile in der Digitalisierung erzielen, die letztendlich nicht nur die digitalen Produkte und Lösungen absichern, sondern auch deren Verkauf aufgrund des gewonnenen Vertrauens steigern. Ich vergleiche Cyber Security immer mit einer Versicherungspolice: Mein Auto fährt auch nicht besser und verbraucht auch nicht weniger Sprit, nur weil es versichert ist. Es muss die Awareness geschaffen werden, dass ohne geeignete Maßnahmen gegen Cyber-Angriffe das Unternehmen sowie sein Ruf sehr stark beschädigt werden können. Cyber Security muss in die Köpfe der Entscheider\*innen getragen werden.

### Sie haben vorhin das Thema Asset Management angeschnitten. Wie wird durch ein gezieltes Asset Management mit Bedrohungsszenarien sowohl präventiv als auch reaktiv umgegangen?

„How can you protect what you don't know?“. Die Implementierung von präventiven Maßnahmen oder die Einführung eines risikobasierten Cyber Security Managements kann nur gelingen, wenn ich Kenntnis über meine Infrastruktur, meine Applikationen und meine Schwachstellen habe. Das Asset Management ermöglicht ein gezieltes Steuern von Maßnahmen für entsprechende Assets wie zum Beispiel das Deployment von Agents, Hardenings oder Releases für gefährdete Systeme. Für eine reaktive Vorfallsbehandlung ist ein gutes Asset Management wichtig, um beispielsweise schnell mit dem Verantwortlichen entsprechende

„Um eine erfolgreiche digitale Transformation zu ermöglichen, muss die Cyber Security ein elementarer Bestandteil des Rahmenwerks sein.“

**Bernd Bauer**

Head of Protection and Consulting Services  
Siemens AG

Gegenmaßnahmen abzustimmen und zu implementieren, um so die Reaktionsgeschwindigkeit zu erhöhen. Deswegen ist Asset Management präventiv sowie auch reaktiv absolut notwendig, um Cyber Security professionell zu betreiben.

#### Welche Rolle spielt das Verständnis der Unternehmens-Assets in der Cyber-Security-Strategie?

Das Verständnis der eigenen Assets spielt eine fundamentale Rolle im Cyber-Security-Kontext. Ein gesamtheitlicher Überblick über IT-/OT-Assets, Special Networks, Business Managed IT-Assets und Cloud-Anwendungen ist notwendig, um geeignete Strategien für die IT-Sicherheit zu ermöglichen. Dabei kann aufgrund der starken Vernetzung der einzelnen Assets untereinander keine gesonderte Betrachtung einzelner Komponenten mehr erfolgen, sondern es ist essenziell, ein ganzheitliches Verständnis zu haben.

#### Gerade das Thema Cloud entwickelt sich aktuell rasant. Gibt es im Asset Management Besonderheiten, die man für Cloud-Plattformen beachten muss?

Asset Management für Cloud-Plattformen ist besonders herausfordernd. Eine zentrale Kontrolle oder eine zentrale Verwaltung von Cloud-Anwendungen muss sicherstellen, dass nur Cloud-Anbieter mit geeigneten Schutzmaßnahmen für die Migration in die Cloud genutzt werden. Als Grundlage muss die Kenntnis darüber bestehen, welche Cloud Accounts vorliegen und genutzt werden. Denn je Cloud Provider habe ich wiederum unterschiedliche Risiko-spezifische Maßnahmen. Im nächsten Schritt ist ein Cloud Compliance Monitoring erforderlich, um zu prüfen, ob die Account Owner Siemens-spezifische Regeln befolgen. Des Weiteren ist ein Cloud Access Security Broker zu etablieren, welcher eine lokale oder Cloud-basierte Software ist, die

zwischen Nutzern und Anwendungen geschaltet ist, sämtliche Aktivitäten überwacht und definierte Richtlinien wie beispielsweise Single Sign-on oder Tokenisierung durchsetzt.

#### Vielen Dank für diesen Überblick, lassen Sie uns gerne diese Themen nachfolgend detaillierter betrachten. Können Sie uns hierzu konkrete Bedrohungsszenarien nennen, zum Beispiel an Schnittstellen zu externen Partnersystemen oder bei der Einbindung von Fremdmaschinen in eine Cloud-Umgebung?

Es muss einem bewusst sein, dass alles, was sich in der Cloud befindet, natürlich gehackt werden kann. Es existieren Angriffsszenarien, in denen eine Cloud-Instanz übernommen wird, um darauf Bitcoin Mining zu betreiben. Das verursacht erhebliche finanzielle Schäden für Unternehmen, die sich nicht im Klaren über eine solche externe Nutzung ihrer Instanzen sind. Durch eine erhebliche Prozessorlast werden so immense Kosten bei Plattformanbietern verursacht. Ein anderes Beispiel könnte ein Angriff auf ein Manufacturing Execution System (MES) sein, das in der Cloud gehostet wird. Das kann zu einem Stillstand in einer oder auch mehreren Fabriken führen.

#### Was sind wichtige Faktoren für ein erfolgreiches Cyber-Security-Konzept bei Cloud-Plattformen? Und existieren nach Ihrer Erfahrung spezifische Bedingungen bei der Nutzung von Cloud-Plattformen in der Manufacturing-Branche?

Der Kern für eine sichere Cloud-Plattform ist eine zentrale Verwaltung und ein einheitliches Regelwerk für die Anwendung von Cloud-basierten Use Cases. Je nach Wichtigkeit der vorliegenden Informationen oder der Applikation bezüglich Verfügbarkeit und Integrität müssen gewisse Schutzmaßnahmen getroffen werden. Die Cloudifizierung

ist ein dynamisches Umfeld, das sich ständig verändert. Microsoft Azure, AWS und Google Cloud entwerfen immer neue Services, die mit anderen Schutzmaßnahmen geschützt werden müssen. Meiner Meinung nach kann die Sicherheit von Cloud-Plattformen nur durch eine zentrale Kontrolle und zentrale Transparenz gewährleistet werden und wenn ein Cloud Security Monitoring durchgeführt wird sowie Schwachstellen kontinuierlich identifiziert und strukturiert abgearbeitet werden. An sich würde ich generell keinen Unterschied zwischen IT- und OT-Anwendungen in einem Werk machen. Es gelten die gleichen Regeln für Cyber Security. Beide unterliegen den gleichen Schutzprinzipien und entsprechenden Konzepten.

Eine wesentliche Herausforderung ist, dass die OT-Welt in der Regel noch nicht den gleichen Reifegrad wie die IT-Welt erreicht hat. Maßgeblich für das Level der Cyber-Sicherheit ist der Grad der Digitalisierung der entsprechenden Fabrik. Bei hochautomatisierten Produktionen wie bei Automobilherstellern besteht eine starke Vernetzung zwischen den Maschinen im Shopfloor, dem MES, SAP-, Warehouse-Management- und angehängten Logistiksystemen. Hier ist es eine komplexe Aufgabe, ein durchgängiges Cyber-Security-Konzept zu realisieren. Zusätzlich muss stark auf die Awareness in solchen Produktionen gepocht werden, da Werksleitende in der Regel durch Produktivität, Verfügbarkeit und Kosten getrieben sind und somit dem Thema der IT-Security oftmals nicht genug Beachtung schenken.

**Wenn wir uns die Entwicklungen der zurückliegenden Jahre vor Augen führen und die immer schnellere digitale Transformation berücksichtigen, welche drei Trends sollte man Ihrer Meinung nach in den nächsten Jahren im Bereich Cyber Security unbedingt beachten?**

Zum einen gibt es durch den höheren Grad von Digitalisierung immer mehr Angriffsvektoren und Tools, die für Cyber-Angriffe wie Hacking genutzt werden. In unserem Konzernprogramm Factory Digitalization stellen wir in enger Abstimmung mit unseren Business Units sicher, das Security by Design maßgeblich bei der Digitalisierung von Produktionsabläufen von Anfang an Anwendung findet, um ein nachträgliches, teures Aufrüsten von Cyber-Security-Maßnahmen zu vermeiden. Zusätzlich ist die Cloudifizierung, also die Verschiebung von On-Premises-Informationen in die Cloud, eine große Herausforderung für die Cyber Security. Bei Siemens wird es beispielsweise ein Programm geben, mit dem sämtliche SAP-Systeme in eine Cloud-Umgebung migriert werden. Hierbei ist es notwendig, die Migration kontrolliert und strukturiert durchzuführen sowie ein Stück der Verantwortung an den Cloud Provider zu übergeben. Ein wesentlicher Aspekt ist hierbei die Sicherstellung der Eignung eines Cloud Providers für die sichere Verwahrung der Firmendaten. Ein dritter Aspekt ist die Product Security an sich. Ein Teil von Digitalisierung betrifft die immer größere Anzahl an digitalen Komponenten in den Produkten.

**In der Industrie ist der Begriff Zero Trust mittlerweile stark verbreitet. Wie wird mit dem Thema Zero Trust bei Siemens umgegangen?**

Wir haben Zero Trust in ein konzernweites Programm eingebettet. Dafür werden Building Blocks erstellt, die über die gesamte Organisation ausgerollt werden, mit dem Ziel, das Intranet zukünftig abzuschalten und die vorhandenen Inhalte in das Internet zu verschieben. Anschließend ist es von großer Bedeutung, dass die Kommunikation zwischen den Devices der Assets oder Applikationen kontrolliert wird. Die Umsetzung wird jedoch noch einige Zeit und Ressourcen benötigen. Siemens ist in diesem Thema ein Vorreiter, bis zu einer vollständigen Umsetzung im Gesamtkonzern wird es aufgrund der Komplexität des Themas aber noch einige Zeit dauern.

**Können Sie uns einen Einblick geben, was elementare Rollen im Cyber-Security-Umfeld sind?**

Eine zentrale Rolle nimmt ein Empowered Cyber Security Officer ein. Man benötigt starke und akzeptierte Persönlichkeiten in der Zentrale und in den Einheiten, damit Cyber Security im täglichen Geschäftsablauf integriert wird. Wichtig ist dabei, dass auf Leitungsebene eine Akzeptanz für diese Rolle und die Verantwortung hinter Cyber Security besteht. Darüber hinaus ist es wichtig, speziell bei einem international agierenden Konzern wie Siemens, dass entsprechende Rollen ebenfalls in Ländern wie China, Indien oder den USA vorgesehen werden, um ein Cyber-Security-Ökosystem in horizontaler und vertikaler Richtung zu ermöglichen und diese in kritische Entscheidungen einzubinden.

**Wie ist der Bereich Cyber Security in der Organisation bei Siemens verankert? Kann man das Thema als vorstandsnah bezeichnen?**

Cyber Security ist innerhalb der Siemens AG äußerst vorstandsnah angesiedelt. Cedrik Neike, der Vorstand von Siemens Digital Industries, dem Digitalisierungstreiber innerhalb des Konzerns, ist ebenfalls verantwortlicher Leiter für den Bereich Cyber Security. Er betont stets, dass es keine Digitalisierung ohne Cyber Security geben kann.

**In der Industrie ist es weithin gängige Praxis, den Bereich Cyber Security in der Unternehmens-IT zu verankern. Warum ist man bei Siemens davon abgewichen?**

IT und Cyber Security stehen im dauerhaften Interessenkonflikt. Für die IT stehen beispielsweise User Experience und Kosten im Vordergrund. Im Bereich Cyber Security hingegen sind Schutzmaßnahmen wie die Integration von Sicherheits-

software oder die aufwendige lückenfreie Dokumentation von Firewall-Infrastrukturen priorisiert zu realisieren. Wir haben uns daher bewusst entschieden, IT und Cyber Security zu trennen, da unsere Erfahrung zeigt, dass im Fall von Kostendruck und Sparprogrammen im Bereich IT oftmals die Maßnahmen hinsichtlich IT-Sicherheit in der Vergangenheit vernachlässigt wurden. Dieses Vorgehen wird mittlerweile auch von vielen Beratungsfirmen als Best Practice empfohlen.

**Herr Bauer, können Sie uns abschließend noch Ihre Key Message für die Entwicklung im Bereich Cyber Security für die nächsten Jahre nennen?**

Cyber Security wird nicht langweilig. Sie wird zukünftig immer wichtiger werden und da die Technologien und Angreifenden sich immer weiterentwickeln, müssen wir als Verteidiger immer agiler sein, um bestmöglichen Schutz zu ermöglichen. Die Weiterentwicklung von Schutzmechanismen wird in den nächsten zehn Jahren sicherlich noch viele Anstrengungen benötigen.

**Herr Bauer, wir danken Ihnen ganz herzlich für Ihre interessanten Einblicke und das offene Gespräch.**

## 2.3 Präventive Risikobehandlung

### Passwortsicherheit hat noch Potenzial

84 Prozent der Teilnehmenden gaben an, die Passwortsicherheit als präventive Maßnahme einzusetzen. Das ist zwar ein hoher Wert, aber gemessen daran, wie einfach Passwortsicherheit umgesetzt werden kann und wie wichtig sie für den Schutz vor Cyber-Angriffen ist, ist dennoch erstaunlich, dass nicht alle Unternehmen diese präventive Maßnahme ergreifen. Eng mit der Passwortsicherheit verbunden ist die Multi-Faktor-Authentifizierung – ein Passwort wird dabei durch einen oder mehrere zusätzliche Faktoren ergänzt oder in speziellen Fällen sogar ersetzt. Für Unternehmen, die Zahlungsverkehr abwickeln, ist diese Methode seit 2021 Pflicht. Im Rahmen unserer Befragung gaben 70 Prozent der Teilnehmenden an, dass diese Methode in ihrem Unternehmen zum Einsatz kommt. Wie beim Thema Passwortsicherheit besteht auch hierdurch die Möglichkeit, die präventiven Maßnahmen zu erweitern. Weit verbreitet sind als prä-

ventive Maßnahmen außerdem der Schutz vor Malware (79%), Back-up-Strategien (78%) und Segmentierung (72%). Auffällig ist, dass bei 23 Prozent der Befragten eine abgesicherte E-Mail-Kommunikation nicht zu den präventiven Maßnahmen gehört – und das, obwohl die Datenkategorie Kommunikationsdaten am dritthäufigsten Ziel von Angriffen ist.

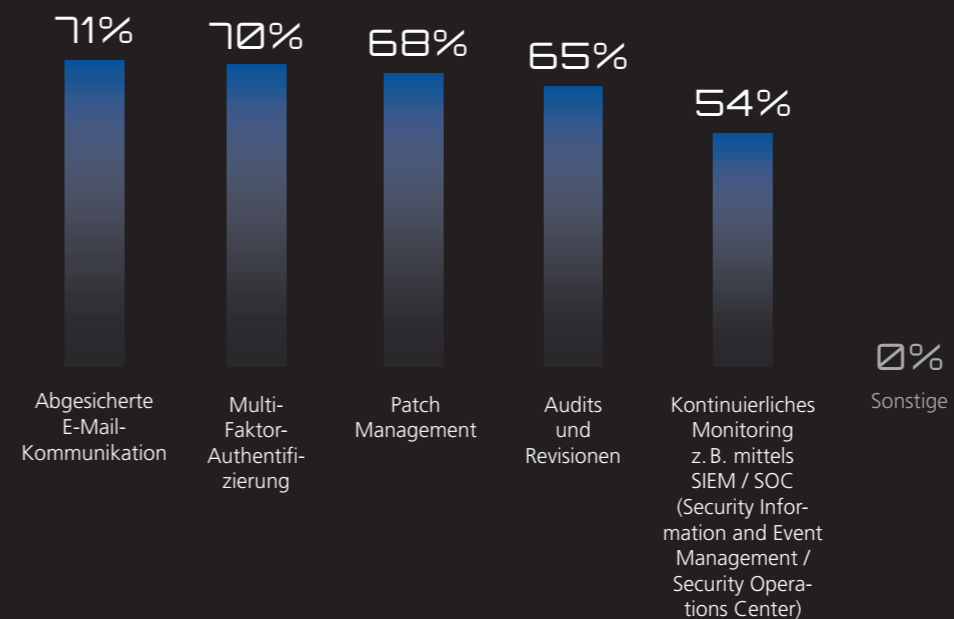
Bei nur gut der Hälfte der Unternehmen kommen die Simulation eines Angriffs (52%), ein kontinuierliches Monitoring (54%) und Kryptografie (54%) zum Einsatz. Generell ist festzustellen, dass die abgefragten präventiven Maßnahmen mit steigender Unternehmensgröße verstärkt Anwendung finden. Ausgehend von der Einschätzung des LKAs ist eine mögliche Erklärung hierfür, dass mit zunehmender Unternehmensgröße auch die zur Verfügung stehenden Ressourcen steigen und gesonderte Abteilungen mit Expert\*innen-Know-how vorhanden sind.

### Welche präventiven Maßnahmen kommen in Ihrem Unternehmen zum Einsatz?

(Auswahl der häufigsten Antworten / Mehrfachauswahl möglich)



Unter **präventiver Risikobehandlung** wird das Management von Risiken verstanden. Das Ziel ist es, IT-sicherheitsrelevante Risiken durch die Planung, Implementierung sowie Optimierung technischer und organisatorischer Maßnahmen zu minimieren.





Unter **Security Awareness** werden alle Aktivitäten zum Aufbau von Wissen bei den Mitarbeitenden und zur Förderung einer Sicherheitskultur verstanden. Ziel ist es, die physischen und informativen Vermögenswerte des Unternehmens zu schützen. Hierunter fallen Maßnahmen, um für die IT-Sicherheit zu sensibilisieren und die verursachten Schäden zu minimieren.

### Normen und Pläne finden Anwendung in Unternehmen

Am häufigsten wird die Norm ISO 27001 (49 %) und am zweithäufigsten die IEC 62443 (27 %) von den Unternehmen genutzt. Orientierung bietet auch der BSI-Grundschutz (23 %). Dagegen werden spezifische Normen, welche einen starken wirtschaftsbereichsabhängigen Bezug aufweisen, deutlich weniger genannt. Interessant ist, dass manche wirtschaftsbereichsspezifischen Normen, beispielsweise die ISO 21434 mit starkem Automotive-Fokus, auch von Unternehmen aus anderen Wirtschaftsbereichen eingesetzt werden – die ISO 21434 vor allem von Unternehmen aus der IT-Branche (27 %).

88 Prozent der befragten Unternehmen gaben an, mindestens einen der Pläne für folgende Zwecke vorliegen zu haben: Meldung eines Vorfalls, Reaktion auf Vorfälle, Aufrechterhaltung des IT-Betriebs sowie Wiederanlauf der IT-Systeme. Befragt wurden die Teilnehmenden auch danach, in welcher Form die Pläne vorliegen. Lediglich 57 Prozent der Unternehmen verfügen über analoge Pläne. Das ist kritisch, da bei Eintritt eines Angriffs durch beispielsweise die Verschlüsselung von Daten der Zugriff auf die Pläne in digitaler Form nicht mehr gewährleistet ist.

### Welche Pläne liegen für den Eintritt eines Vorfalls vor?

(Mehrfachauswahl möglich)



### Vermittlung von Inhalten zur IT-Sicherheit ist keine Selbstverständlichkeit

Zwar schulen 85 Prozent der befragten Unternehmen alle Mitarbeitenden in den Grundlagen der IT-Sicherheit, immerhin 14 Prozent machen das aber nicht. Spezifische Inhalte werden bei 78 Prozent der Unternehmen an IT-Systemverantwortliche vermittelt, in 76 Prozent an Anwender\*innen von besonders kritischen IT-Systemen, in 72 Prozent an IT-Führungskräfte und in 64 Prozent an alle Führungskräfte. Bei kleinen Unternehmen weichen die Werte deutlich ab: Nur 63 Prozent unterweisen alle Mitarbeitenden in den Grundlagen der IT-Sicherheit. Bei der Vermittlung spezifischer Inhalte liegen ebenfalls sämtliche Werte deutlich unter dem Durchschnitt. Gerade bei kleinen Unternehmen besteht daher noch erheblicher Bedarf, eine Sicherheitskultur zu etablieren.

### Generische statt spezifische Inhalte





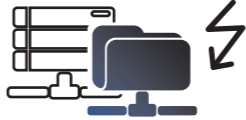



Als Formate werden am häufigsten Unternehmensrichtlinien (60 %), Webinare (53 %) und Präsenzs Schulungen (49 %) genutzt. Innovative Schulungsformate wie integrierte Lernplattformen (40 %) und Planspiele (17 %) kommen derzeit weniger zum Einsatz.

Der Großteil der Unternehmen schult hauptsächlich generische Inhalte wie den Schutz persönlicher Daten (85 %), IT-Sicherheit (84 %) und den Umgang mit externen Datenträgern beziehungsweise E-Mail-Anhängen (82 %). Spezifische Inhalte wie der Umgang mit Sicherheitssoftware (65 %), Social Engineering (59 %) und die private Nutzung von Social Media (57 %) werden hingegen seltener vermittelt. Hier besteht nach unserer Einschätzung noch erheblicher Nachholbedarf. Denn wie in Kapitel 2.2 bereits beschrieben, ist Social Engineering für jeden dritten Angriff mit resultierendem Schaden als Sicherheitslücke verantwortlich. Ergänzend hierzu stellt die Nutzung von Plattformen auf geschäftlichen Endgeräten ein zusätzliches Risiko dar.



# HANDLUNGS- EMPFEHLUNGEN

# 3.0

- 1  Polizeibehörden bei IT-sicherheitsrelevanten Vorfällen informieren und aktiv einbinden
- 2  Zentrale IT-Abteilung umfänglich unterstützen und mit den notwendigen Weisungsbefugnissen ausstatten
- 3  Identifikation von IT-sicherheitsrelevanten Risiken um relevante Aspekte erweitern
- 4  Aufwand zum Schutz von Kommunikationsdaten lohnend, Optimierungspotenzial bei Daten zur Unternehmensstrategie heben
- 5  Verbindungen zwischen Back-ups und anderen IT-Systemen vermeiden
- 6  Passwortsicherheit als schnell umzusetzende Maßnahme etablieren und kontinuierlich verbessern
- 7  Cyber-Security-Awareness und das IT-Security-Bewusstsein der Mitarbeitenden unter anderem durch Schulungen oder Kampagnen steigern
- 8  Bei Cyber-Security-Awareness hohe Aufmerksamkeit auf Social Engineering legen

## Handlungsempfehlungen im Detail

### 1. Polizeibehörde bei IT-sicherheitsrelevanten Vorfällen informieren und aktiv einbinden

Unternehmen wenden sich bei einem IT-sicherheitsrelevanten Vorfall häufig nicht an die entsprechende Polizeibehörde. Dabei können die polizeilichen Erfahrungswerte, über die Aufnahme der Strafanzeige hinaus, dahingehend genutzt werden, dass durch zielgerichtete forensische Analysen Täter\*innen und Vorgehen erkannt werden. Das einzelne Unternehmen kann dies beispielsweise für einen schnellen Wiederaufbau der IT-Systeme nutzen. Hinzu kommt, dass Unternehmen oftmals vor einer falschen Herangehensweise bei der Wiederherstellung von Back-up-Daten bewahrt werden, wenn sie die Unterstützung der Polizeibehörde in Anspruch nehmen. Auch wenn in einem konkreten Fall dem betroffenen Unternehmen nicht direkt geholfen werden kann, so können, aufgrund exklusiver rechtlicher Befugnisse und technischer Mittel, oftmals viele andere Unternehmen, die bereits im Visier der gleichen Angreifenden sind, vor einer unmittelbar bevorstehenden Attacke gewarnt werden.

### 2. Zentrale IT-Abteilung umfänglich unterstützen und mit den notwendigen Weisungsbefugnissen ausstatten

Die zentrale IT-Abteilung ist meist hauptverantwortlich für die Identifikation von Cyber-Security-Risiken. Sie ist somit die erste Stelle, die bei einem Vorfall informiert wird und reaktive Maßnahmen einleitet. Um diese essenzielle Rolle wahrnehmen zu können, muss die Abteilung beziehungsweise die IT-Leitung über die erforderliche Weisungsbefugnis verfügen. In gleichem Maß wichtig ist, dass passende Ressourcen zur Verfügung stehen, um die richtigen Kompetenzen im Team sicherzustellen. Ein weiterer Erfolgsfaktor ist die Budgetverfügung für die Unterstützung der Abteilung durch IT-Sicherheitsexpert\*innen. Dabei ist sicherzustellen, dass eine Beauftragung bei Eintritt eines Vorfalls besonders schnell erfolgen kann.

### 3. Identifikation von IT-sicherheitsrelevanten Risiken um relevante Aspekte erweitern

Um das Risiko von Cyber-Security-Vorfällen im Unternehmen zu senken, ist die Durchführung einer Risikoanalyse essenziell. Der erste Schritt zur effektiven Analyse von IT-sicherheitsrelevanten Risiken ist deren Identifikation. Dabei gibt es eine Reihe von Aspekten, die zu berücksichtigen sind; etwa Angriffsziele, Angriffspfade, Angriffswerkzeuge, potenzielle Angreifende sowie aktuelle Informationen über die generelle Bedrohungslage im Land und im jeweiligen Wirtschaftsbereich. Diese Aspekte werden von vielen Unternehmen jedoch nicht vollumfänglich betrachtet. Aus diesem Grund ist ein Review der Aspekte, die im Unternehmen zur Risikoidentifikation in Betracht gezogen werden, durchzuführen. Bei Bedarf sollten zusätzliche Merkmale mit aufgenommen werden.

### 4. Aufwand zum Schutz von Kommunikationsdaten lohnend, Optimierungspotenzial bei Daten zur Unternehmensstrategie heben

Kommunikationsdaten (z.B. Kontaktdaten und Inhalte von E-Mails) sind am dritthäufigsten Ziel von Angriffen und sollten daher auch weiterhin mit entsprechend großem Aufwand gesichert werden. Dies ist vielen Unternehmen bereits bewusst. Daten zur Unternehmensstrategie sind dagegen seltener im Fokus – obwohl auch diese häufig das Ziel von Angriffen sind. Diese Datenkategorie besser abzusichern, birgt für viele Unternehmen ein erhebliches Optimierungspotenzial. Möglichkeiten sind die Überprüfung der Datenablage zur Unternehmensstrategie sowie eine regelmäßige Kontrolle der Zugriffsrechte.

### 5. Verbindungen zwischen Back-ups und anderen IT-Systemen vermeiden

Ein Network Attached Storage (NAS) als Back-up zu nutzen, ist riskant – zum Beispiel kann bei einer Ransomware-Attacke auch ein NAS betroffen sein; die Wiederherstellung wichtiger Daten ist dann nicht mehr möglich. Denn werden die Unternehmensdaten bei einem solchen Angriff verschlüsselt, ist auch das Back-up nicht mehr nutzbar. Geeignete Back-up-Strategien sollten daher grundsätzlich die Sicherungen auf unterschiedlichen Medien beinhalten und eine Verbindung mit anderen IT-Systemen vermeiden. Die Lagerung sollte im Optimalfall an einem anderen Ort erfolgen, um die Daten auch vor natürlichen Gefahren wie Feuersbrüchen effektiv zu schützen.

### 6. Passwortsicherheit als schnell umzusetzende Maßnahme etablieren und kontinuierlich verbessern

Hacker\*innen verwenden häufig Werkzeuge, die automatisiert Zeichenkombinationen für Passwörter testen, oder sie kaufen Daten im Internet, um sich Zutritt zu digitalen Diensten zu verschaffen. Um dies bestmöglich zu verhindern, sollten Passwörter bestimmte Qualitätsanforderungen erfüllen, regelmäßig geändert und idealerweise lediglich für einen Zugang genutzt werden.

Als weitere präventive Maßnahme zur Passwortsicherheit ist die Multi-Faktor-Authentifizierung zu nennen. Dabei wird das Passwort durch einen oder mehrere zusätzliche Faktoren ergänzt oder gänzlich ersetzt.

### 7. Cyber-Security-Awareness prägen und das IT-Security-Bewusstsein der Mitarbeitenden steigern

Awareness ist ein elementares Element für die IT-Sicherheit, denn die Mitarbeitenden sind bei Cyber-Angriffen häufig die erste Verteidigungslinie. Menschliches Fehlverhalten und die hierdurch entstehenden Sicherheitslücken führen oftmals dazu, dass Angreifenden unberechtigt Zugang zu einem System ermöglicht wird und gespeicherte Daten ausgespäht oder manipuliert werden. Einfache Awareness-Trainings senken dieses Risiko. Phishing-Angriffe zu simulieren, Passwortsicherheit wirklich anzuwenden und das Bewusstsein für regelmäßige Back-ups zu stärken, sind erste richtige Schritte.

### 8. Bei Cyber-Security-Awareness hohe Aufmerksamkeit auf Social Engineering legen

Wenn sich Personen unberechtigt als Mitarbeitende eines Unternehmens ausgeben und in deren Namen Anweisungen erteilen – beispielsweise per E-Mail zur Überweisung hoher Geldsummen oder zur Herausgabe von internen Informationen –, kann das zu einem bedeutenden Schaden für das Unternehmen führen. Diese Art des Angriffs fällt unter Social Engineering. Vielen Mitarbeitenden ist diese Möglichkeit eines Vorfalls nicht direkt bewusst. Hier besteht daher ein hohes Optimierungspotenzial, da verstärkte Awareness zum Thema Social Engineering das Risiko eines solchen Vorfalls vermindern kann.

„Cyber Security betrifft das gesamte Unternehmen von der Strategie über die Organisation bis hin zum operativen Tagesgeschäft. In einer zunehmend digitalen Welt hat der Schutz von Daten als wertvolles und sensibles Gut oberste Priorität.“

**Markus Wambach**

Member of the Board of Management  
MHP – A Porsche Company

„Cyber Security muss einhergehen mit Digitalisierung.“

**Bernd Bauer**

Head of Protection and Consulting Services  
Siemens AG

„In den zurückliegenden Jahren kann man feststellen, dass ein Anstieg der Sensibilität stattgefunden hat und das Thema in deutschen Unternehmen zunehmend ernst genommen wird.“

**Rudolf Näher**

Leiter der Zentralen Ansprechstelle Cybercrime (ZAC)  
Landeskriminalamt Baden-Württemberg



# FAZIT UND AUSBLICK

# 4.0

Die zunehmende Digitalisierung bietet deutschen Unternehmen enorme Chancen. Der Cyber-Security-Risk-Report 2021 zeigt jedoch, dass durch die steigende Vernetzung und Datengenerierung im gleichen Maß neue Risiken entstehen. Es wird deutlich, dass viele Unternehmen von IT-sicherheitsrelevanten Vorfällen betroffen sind, die diverse Auswirkungen haben und einen enormen Schaden verursachen. Eine umfassende Risikobetrachtung bleibt dennoch mehrheitlich aus, die Unterstützung durch Behörden wird nicht in vollem Ausmaß genutzt.

Vor diesem Hintergrund ist es enorm wichtig, dass sich Unternehmen unabhängig von ihrer Größe frühzeitig mit der IT-Sicherheit beschäftigen. Es reicht nicht, Notfallpläne nur vorliegen zu haben. Diese müssen auch sämtliche Aspekte abdecken, stets aktuell sein, kontinuierlich validiert werden und analog zugänglich sein. Zur zielgerichteten Umsetzung der Notfallpläne benötigen IT-Abteilungen die notwendige Befugnis für eine schnelle Reaktion. Aus präventiver Sicht ist eine hohe Awareness der Mitarbeitenden unverzichtbar, da sie oft das Einfallstor für Angriffe sind. Besonderen Schutz sollten Verwaltungs- und Personaldaten, Finanzkennzahlen und Kommunikationsdaten erhalten, da sie besonders wertvoll sind und ein häufiges Ziel darstellen. Neben den zu ergreifenden internen Maßnahmen ist für eine umfassende Cyber Security wichtig, Polizeibehörden zu vertrauen sowie einzubeziehen, um somit präventive und repressive Maßnahmen umfassend zu ermöglichen. Eine intensive Zusammenarbeit kann für angegriffene und noch nicht angegriffene Unternehmen zu erhöhtem Schutz beitragen.

Sowohl die Ergebnisse der Umfrage als auch die Aussagen der Interviewpartner zeigen auf, dass Cyber Security in den kommenden Jahren immer wichtiger wird. Die Digitalisierung hält für die Zukunft noch unzählige Innovationen bereit. Daraus resultieren aber auch zahlreiche Herausforderungen und potenzielle Schwachstellen für Unternehmen. Beides macht neugierig und lässt uns mit Spannung auf die kommenden Jahre blicken.

**An dieser Stelle möchten sich die Autor\*innen bei allen Teilnehmenden für ihre Antworten sowie bei den Experten für die gute Zusammenarbeit mit dem Landeskriminalamt Baden-Württemberg und MHP herzlich bedanken.**

## ANSPRECHPARTNER

### Andreas Henkel

Associated Partner

MHP Focus Topic Lead Cyber Security  
MHP – A Porsche Company  
andreas.henkel@mhp.com  
+49 151 40 66 75 26



### Frank Winterhalter

Leiter der Führungsgruppe  
Cybercrime und Digitale Spuren,  
Landeskriminalamt  
Baden-Württemberg  
stuttgart.lka.abt5@polizei.bwl.de  
+49 711 54 01 25 01



### Kitty Wanke

Senior Management Consultant  
MHP – A Porsche Company



### Frank Cichon

Senior Management Consultant  
MHP – A Porsche Company



### Sebastian Klüh

Senior Management Consultant  
MHP – A Porsche Company



## AUTOR\*INNEN

### Pascal Barreuther

Management Consultant  
MHP – A Porsche Company



### Sven Halusa

Management Consultant  
MHP – A Porsche Company



ENABLING YOU  
TO SHAPE A BETTER  
TOMORROW >>>

#### Bildrechte ©by Adobe Stock

Cover Jackie Niam // Seite 2/3 your123 // Seite 8/9 metamorworks // Seite 10 kerkezz //  
Seite 11 Kabardins photo // Seite 12 luckybusiness // Seite 30 Robert Daly/Caia Image //  
Seite 46 Gajus // Seite 50/51 Вадим Пастух // Seite 56/57 Shutter2U

Weitere Bildrechte: Seite 22/23 ©Reise // Seite 39 Portrait ©by K Renter

Layout  
Freiland Design

# MHP: DRIVEN BY EXCELLENCE

20 MHP Offices in Germany, England, USA, China,  
Romania, Czech Republic, Austria, Israel, and Hungary.



## Germany

Ludwigsburg  
(Headquarters)  
Berlin  
Düsseldorf  
Frankfurt a. M.  
Ingolstadt  
Munich  
Nuremberg  
Wolfsburg

## International

Atlanta (USA)  
Reading (England)  
Cluj-Napoca (Romania)  
Timișoara (Romania)  
Prague (Czech Republic)  
Shanghai (China)  
Zell am See (Austria)  
Tel Aviv (Israel)  
Budapest (Hungary)