VDMA Studie

Industrial Security und Produktpiraterie 2024

Hinweis

Selbstverständlich haben wir die Angaben der Teilnehmenden mit der gewohnten Diskretion behandelt. In den folgenden Kapiteln finden Sie deshalb die Ergebnisse in anonymisierter und zusammengefasster Form wieder. Sollten Sie für die nächste Studie zu Industrial Security und Produktpiraterie noch weitere Anregungen oder Fragen zur Auswertung haben, dann nehmen Sie bitte mit uns Kontakt auf.

RA Dr. Friedrich-Philipp Becker
Rechtsanwalt (Syndikusrechtsanwalt) / Gewerblicher Rechtsschutz,
IT-Recht, Urheberrecht, UWG
Tel: +49 69 6603-1309
E-Mail: friedrich-philipp.becker@vdma.org

Holger Paul
Leiter Kommunikation
Tel: +49 69 6603-1922
E-Mail: Holger.Paul@vdma.org

Steffen Zimmermann
Leiter Competence Center Industrial Security
Tel: +49 69 6603-1978
E-Mail: Steffen.Zimmermann@vdma.org

VDMA
Lyoner Str. 18
60528 Frankfurt am Main

www.vdma.org

Stand: 10.04.2024

Inhaltsverzeichnis

1 Einführung

Der VDMA führt alle zwei Jahre eine Studie zum Thema Produkt- und Markenpiraterie unter den Mitgliedsunternehmen durch. Bereits seit über 20 Jahren werden somit verlässliche Zahlen und Informationen gesammelt, um der Bedrohung durch Plagiate, Fälscher und Kopierer in unserer Branche ein Bild zu geben. In diesem Jahr wurde die Studie erstmals um das Themenfeld Industrial Security erweitert, um dem Umstand der gestiegenen digitalen Vernetzung in den Produkten und den verbundenen digitalen Bedrohungen für den Maschinen- und Anlagenbau Rechnung zu tragen. Dies bestätigen die Umfrageergebnisse: 96 Prozent der befragten Unternehmen setzen Cybersecurity-Maßnahmen zur Absicherung ihrer Betriebsstätte gegen Angriffe ein. Im Zuge dessen sind einzelne Fragen zum Themenbereich Produktpiraterie entfallen, um den Fragebogen noch in einer bearbeitbaren Größe zu halten.

Definition Produktpiraterie

Die Studie bezieht sich allein auf den unzulässigen Nachbau. Unter dem unzulässigen Nachbau (hier gleichbedeutend als Produktpiraterie bzw. Plagiat bezeichnet) wird der

- Nachbau unter Verletzung von Sonderschutzrechten (z. B. Marken, Patente) oder
- ohne Verletzung von Sonderschutzrechten, aber das Urheberrecht verletzende und/oder in wettbewerbswidriger Weise erfolgte Nachbau

verstanden. Der Nachbau erfolgt dann in wettbewerbswidriger Weise, wenn neben der Nachahmung zusätzlich noch eine unlautere Handlung eintritt. Diese unlautere Handlung ist in der Regel eine Täuschung über den Hersteller der Originalware (Verwechslungsgefahr) und die damit verbundene Ausnutzung des guten Rufs.

Definition Industrial Security

Industrial Security ist der Schutz technischer Systeme in Produktion, Fertigung und Intralogistik vor prinzipiell unbekannten Angriffen und Störungen mit dem Ziel, den Geschäftsprozess im Betrieb aufrecht zu erhalten. Als technische Systeme gelten dabei Maschinen und Anlagen, deren industrielle Steuerungskomponenten, Netzwerkkomponenten, Sensoren und Aktoren sowie die mit den Systemen verbundenen Dienste.

Ursache von Angriffen und Störungen technischer Systeme sind Menschen oder die Umgebung des Systems (Umwelt). Zum besseren Verständnis lässt sich dies auf „Schutz der Maschine vor dem Menschen“ reduzieren.

Industrial Security ist als Prozess zu verstehen, der den Schutz vor Ausfall, Know-how-Abfluss, Spionage sowie Manipulation von Maschinen, Anlagen und Industriedaten sicherstellen soll. Security-Vorfälle aus dem „Office-Umfeld“ (IT-/Cybersecurity) sind zusätzlich von Relevanz, wenn sich Auswirkungen auf Maschinen oder Anlagen zeigen.

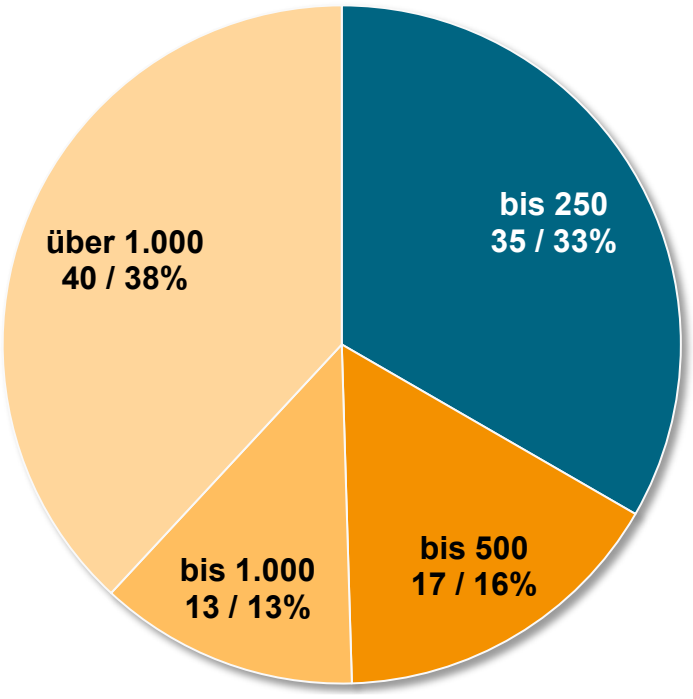
Teilnehmendenstruktur 2024

Dieses Jahr haben sich im Zeitraum der Datenerhebung von Anfang bis Ende Februar 105 Mitgliedsunternehmen des VDMA an der Studie zu Industrial Security und Produktpiraterie beteiligt. Im Vergleich zur letzten Studie im Jahr 2022 ist die Anzahl der Teilnehmenden damit von 68 wieder deutlich angestiegen, was zu Teilen an der Erweiterung um den Themenbereich Industrial Security liegen mag.
Naturgemäß schwankt die Stichprobengröße pro Frage, da nicht alle Teilnehmenden zu allen Fragen eine Antwort abgeben. Daher ist die jeweilige Stichprobengröße bei den einzelnen Fragen angegeben.

Im Vergleich zur letzten Studie ist die absolute Anzahl der Rückmeldungen, die kleinen und mittleren Unternehmen zuzuordnen sind, weitestgehend identisch geblieben. Ihr Anteil verringert sich damit deutlich um 13 Prozentpunkte auf 33 Prozent. Der Großteil der zusätzlichen Rückmeldungen verteilt sich auf Unternehmen mit mehr als 250 Mitarbeitenden. Während der prozentuale Anteil von Unternehmen mit mehr als 1.000 Mitarbeitenden weitestgehend identisch bleibt (+1 Prozentpunkt), treten Unternehmen mit Mitarbeitendenzahlen zwischen 250 und 1.000 damit stärker in Erscheinung.

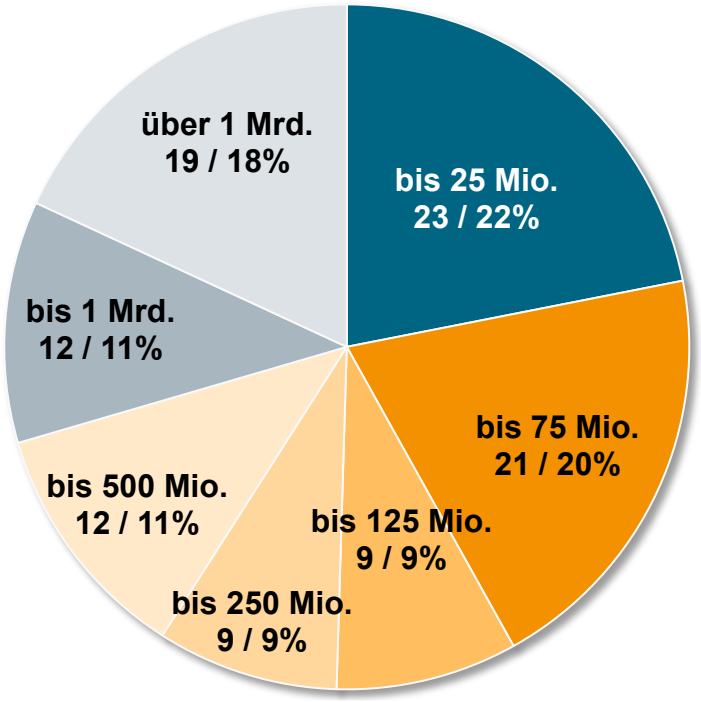
Die genaue Teilnehmendenstruktur nach Anzahl der Mitarbeitenden und Jahresumsatz kann den folgenden beiden Grafiken entnommen werden.

Teilnehmendenstruktur der Studie nach Anzahl der Mitarbeitenden



Aufteilung der Studienteilnehmenden nach Anzahl der Mitarbeitenden. N=105

Teilnehmendenstruktur der Studie nach Jahresumsatz



Aufteilung der Studienteilnehmenden nach Jahresumsatz. N=105

2 Management Summary

In diesem Jahr wurde die Studie zur Produktpiraterie erstmals um Fragen aus dem Themenbereich Industrial Security erweitert. .

Die befragten Unternehmen melden ein Rekordtief an Betroffenheit von Produkt- und/oder Markenpiraterie: **46 Prozent der befragten Unternehmen im deutschen Maschinen- und Anlagenbau gaben an, von Produkt- oder Markenpiraterie betroffen zu sein**. Während damit immer noch rund jedes zweite Unternehmen betroffen ist, bedeutet dies einen **Rückgang um 26 Prozentpunkte**. Ein erfreuliches Signal, nachdem in der vergangenen Studie ein deutlicher Zuwachs an ergriffenen Maßnahmen zu verzeichnen war. Möglicherweise wurde dieser Rückgang zusätzlich dadurch verstärkt, dass mit Aufnahme des neuen Themenbereichs Industrial Security Unternehmen zur Teilnahme motiviert wurden, für die zwar Industrial Security von hohem Stellenwert ist, die aber nicht von Produktpiraterie betroffen sind.

Die hohe Relevanz von Industrial Security zeigt sich auch in den Antworten: **96 Prozent der Befragten sichern ihre Betriebsstätte mit mindestens einer Cybersecurity-Maßnahme ab.** Zusätzlich haben 59 Prozent eine Cyberversicherung abgeschlossen, die von 6 Prozent der Befragten auch bereits in Anspruch genommen werden musste.

Dies spiegelt sich auch in der Bereitschaft der Unternehmen wider, sich in lokalen oder regionalen **Cyberbündnissen** zu engagieren: **13 Prozent engagieren sich bereits, 50 Prozent können sich ein Engagement grundsätzlich vorstellen.**

Entsprechend zum Rückgang der Betroffenheit von Produkt- oder Markenpiraterie fällt im Vergleich zu den vergangenen Studien auch der hierdurch entstandene Schaden deutlich: **der geschätzte Schaden beläuft sich auf 4,1 Milliarden Euro jährlich und ist damit 2,3 Milliarden Euro niedriger als zuletzt.** Ein Umsatz in dieser Schadenshöhe würde der Branche knapp 16.000 Arbeitsplätze sichern.

Als Herkunftsland von Plagiaten behauptet sich erneut die Volksrepublik China mit 82 Prozent als unangefochtener Platzhirsch. Trotz eines Rückgangs der Nennungen bleibt Deutschland mit 16 Prozent, wie zuletzt, hinter Indien mit 18 Prozent auf Platz drei der Herkunftsländer.

Plagiate bleiben ein stetiges Sicherheitsrisiko

Plagiate können nachweisbar ein Sicherheitsrisiko darstellen: **zwei von drei Unternehmen berichten, dass von Plagiaten ihrer Produkte Gefahren ausgehen.** Rund jede zweite Fälschung birgt eine Gefahr für die Anlage, und **in 40 Prozent der Fälle für den Menschen, beispielsweise den Bediener einer Anlage.**

Hilfe: Leitfaden und Normen als erste Informationsquelle

VDMA-Hilfen zum "Produkt- und Know-how-Schutz", zu „Maßnahmen auf Messen“ und zur „Industrial Security“ bieten betroffenen Unternehmen Unterstützung bei der Auswahl und Umsetzung geeigneter Schutzmaßnahmen. Weitere Informationen finden Sie dazu in der aktuellen Publikationsliste am Ende der Studie.

Die wichtigsten Ergebnisse der VDMA Studie Industrial Security und Produktpiraterie 2024:

- **Rund jedes vierte Unternehmen war in den vergangenen beiden Jahren von einem signifikanten Cybersecurity-Vorfall betroffen.**
- **96 Prozent der Befragten sichern ihre Betriebsstätte mit mindestens einer Cybersecurity-Maßnahme ab.** Neben regelmäßigen Backups und Updates von Betriebssystemen und Anwendungen setzen 80 Prozent der befragten Unternehmen Maßnahmen zur Angriffserkennung ein, um frühzeitig Gegenmaßnahmen einleiten zu können.
- Die Bereitschaft zum Engagement in einem lokalen oder regionalen Cyberbündnis ist hoch: **13 Prozent engagieren sich bereits, 50 Prozent können sich ein Engagement grundsätzlich vorstellen.**
- **46 Prozent der Unternehmen im Maschinen- und Anlagenbau sind von Produktpiraterie betroffen** (2022: 72 Prozent).
- **Der geschätzte Schaden durch Produktpiraterie im Umsatzjahr 2023 betrug 4,1 Milliarden Euro** und verzeichnet damit einen deutlichen Rückgang um 2,3 Milliarden Euro im Vergleich zur Studie von 2022. **Der durchschnittliche Schaden für betroffene Unternehmen sinkt ebenfalls auf 3,5 Prozent des Jahresumsatzes, von zuletzt 4,9 Prozent.**
- Der Umsatzverlust von 4,1 Milliarden Euro entspricht rund 16.000 Arbeitsplätzen (2022: 29.000).
- Die Volksrepublik **China führt mit 82 Prozent deutlich die Liste der Herkunftsländer von Plagiaten an. Auf Platz zwei folgt Indien mit 18 Prozent**, vor Deutschland auf Platz drei (16 Prozent).
- Als Plagiatoren beziehungsweise als Auftraggeber von Plagiaten treten direkte Wettbewerber mit 58 Prozent seltener in Erscheinung als zuvor (2022: 70 Prozent). **Dafür ist bei professionellen Großplagiatoren (42 Prozent) und staatlichen Unternehmen (18 Prozent) mit einem Plus von 40 bzw. 63 Prozent ein deutlicher Zuwachs zu verzeichnen.**
- **Kunden und Zulieferer sind keine relevanten Plagiatoren mehr:** nach zuletzt steigenden Zahlen treten Kunden nur noch mit 6 Prozent in Erscheinung (2022: 26 Prozent) und Zulieferer wurden von keinem Unternehmen genannt.
- Bei den Schutzrechtsverletzungen **verdrängt die Markenpiraterie mit 49 Prozent erstmals den unlauteren Nachbau mit 44 Prozent auf Platz zwei.** Die Verletzung sonstiger Rechte, beispielsweise des Urheberrechts, ist verglichen mit der vergangenen Studie erneut um 9 Prozentpunkte auf nunmehr 37 Prozent angestiegen. **Besonders deutlich ist die Zunahme der Schutzrechtsverletzung von Gebrauchsmustern und Design.**
- Häufigstes Plagiat bleiben in rund 60 Prozent der Fälle die beiden Kategorien „Komponenten“ und „äußeres Erscheinungsbild (Design)“. Seltener kommen sogenannte „weiche“ Plagiate vor (Kataloge, Broschüren, Produktfotos), die erneut auf das Niveau von vor vier Jahren angestiegen sind. **Deutlich zugewonnen haben Plagiate von Websites und Online-Shops, Bedienungsanleitungen und technischen Dokumentationen, Verbrauchsmaterialien, sowie digitalen Dienstleistungen.**
- **Plagiate bleiben nachweisbar ein stetiges Sicherheitsrisiko: 41 Prozent der Unternehmen** berichten von Fälschungen, die eine Gefahr für Bediener oder Anwender mit sich bringen. **Über die Hälfte der Befragten (54 Prozent) sehen bei den entdeckten Plagiaten eine Gefahr für den sicheren Betrieb der Anlage.**

Der VDMA handelt

Produktpiraterie und Cyberangriffe sind eine enorme Bedrohung für die Innovationskraft und Wettbewerbsfähigkeit unserer Industrie. Dabei erweisen sich die Gefahren der Piraterie, des Verlusts von Know-how und Cyberangriffe wie Ransomware im Maschinen- und Anlagenbau als sehr vielgestaltig. Insbesondere durch den digitalen Wandel ergeben sich neue Herausforderungen für den Schutz von Daten und Informationen, sowohl in der Produktentwicklung als auch im Betrieb von Maschinen und Anlagen. Gleichzeitig sind digitale Services und integrierte Schutzmaßnahmen eine gute Möglichkeit, sich mit Mehrwerten von Plagiatoren abzusetzen, den einfachen Nachbau zu erschweren und die Integrität in der Lieferkette sicherzustellen.

Wir raten Unternehmen für einen nachhaltigen Umgang mit Cyberangriffen und Produktpiraterie zu einer umfassenden Abwehrstrategie mit Anpassungen an Unternehmenssituation und individuelle Produktrisiken. Verschiedene, aufeinander abgestimmte Maßnahmen sollten zu einem individuellen Schutzkonzept nach ISO 22384 kombiniert werden („Cyber-Physical Product Security“). Grundsätzlich sollten im Feld der Produktpiraterie rechtliche Schutzvorkehrungen in Form von Schutzrechtsanmeldungen in den jeweiligen Märkten vorgenommen werden. Ohne Schutzrechtsanmeldung ist eine Rechtsdurchsetzung nahezu unmöglich. Ebenso müssen organisatorische und technische Maßnahmen in Betracht gezogen werden, die sowohl die eigenen Mitarbeitenden als auch Zulieferer, Händler oder Kunden miteinbeziehen.

Der VDMA unterstützt seine Mitgliedsunternehmen tatkräftig in den verschiedenen Bereichen:

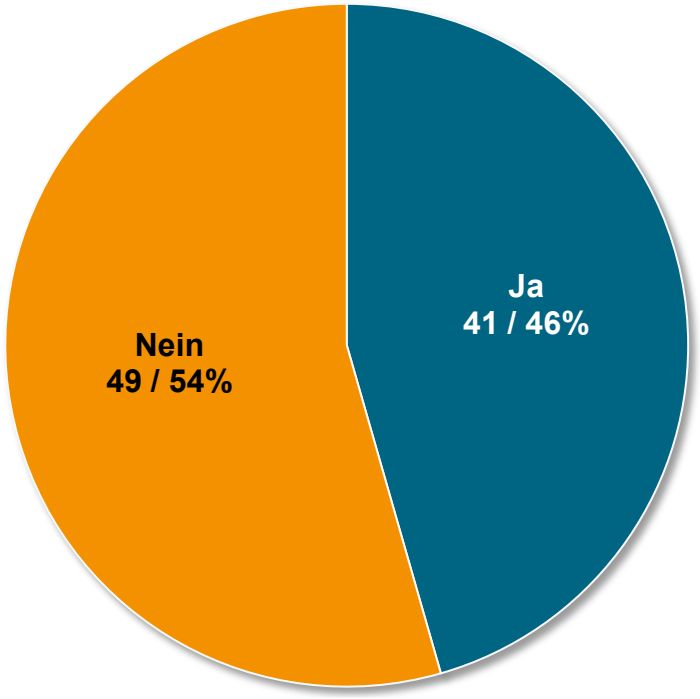
- Die Rechtsabteilung berät und informiert bei juristischen Fragestellungen.
- Der VDMA-Arbeitskreis „Gewerblicher Rechtsschutz“ vernetzt betroffene Mitgliedsunternehmen zu organisatorischen und rechtlichen Maßnahmen.
- Über unsere Büros in Berlin und Brüssel erhöhen wir weiter den Druck in Richtung Bundesregierung und Europäische Union, entschlossener gegen Produktpiraterie vorzugehen.
- Die VDMA-Arbeitskreise „Industrial Security“, „NIS2“ und „Informationssicherheit“ vernetzen Mitgliedsunternehmen zum Erkenntnisgewinn und Erfahrungsaustausch im Feld der digitalen Angriffe und Schutzmaßnahmen.
- Der VDMA hat federführend an der ISO 22384 „Guidelines to establish and monitor a protection plan and its implementation“ mitgewirkt.
- Der VDMA stellt den stellvertretenden Obmann im deutschen Spiegelgremium des ISO/TC 292 „Security and resilience“, dem NIA-02-01 „Maßnahmen zur Echtheit und Integrität von Produkten“.
- Jährliche Anwendertage zu den Themenbereichen "Informationssicherheit (IT/OT)" sowie "Product Security" bieten Mitgliedsunternehmen aktuelle Informationen zur Regulierung, Standardisierung und Einblicke in praxiserprobte Lösungen.

3 Betroffenheit in der Produktpiraterie

Während über die vergangenen Studien hinweg Produktpiraterie eine stete und enorme Bedrohung für die Innovationskraft und Wettbewerbsfähigkeit unserer Branche war, zeigt sich mit dieser Studie erstmals ein **deutlicher Rückgang um 26 Prozentpunkte auf ein historisches Tief von 46 Prozent.** So erfreulich dieser Rückgang auf den ersten Blick ist, zeigt das Ergebnis dennoch, dass **weiterhin jedes zweite befragte Unternehmen von Produkt- und/oder Markenpiraterie betroffen** ist.

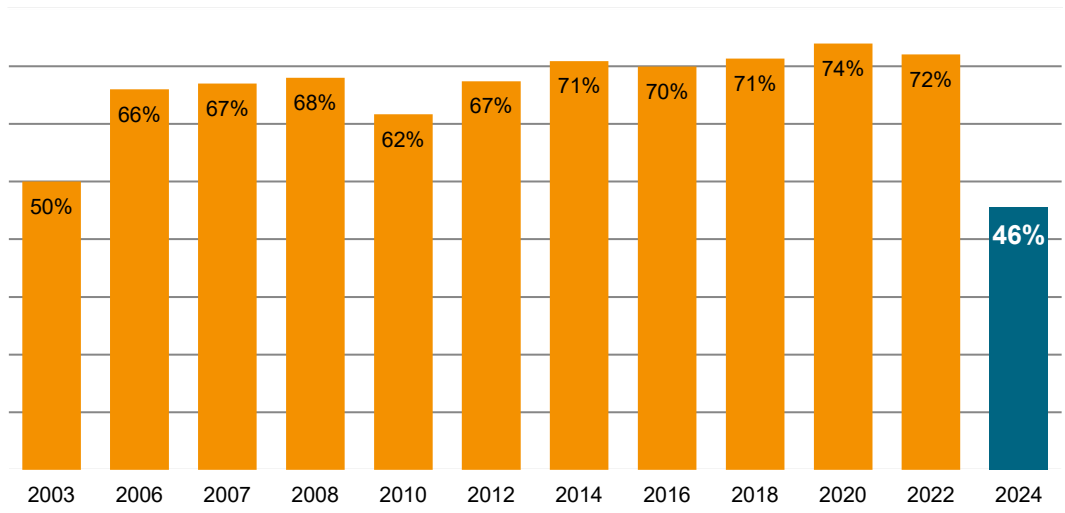
Auf die Ursache dieses Rückgangs gibt die Studie keine direkten Rückschlüsse. Es ist jedoch zu bedenken, dass der Themenbereich Industrial Security erstmals neu in die Studie aufgenommen wurde, was potenziell Unternehmen zur Teilnahme motiviert hat, für die zwar Industrial Security einen hohen Stellenwert hat, die aber nicht von Produktpiraterie betroffen sind.

Ist Ihr Unternehmen von Produkt- und/oder Markenpiraterie betroffen?



Anteil der von Produkt- und Markenpiraterie betroffenen Unternehmen. N=90

Von Produkt- und Markenpiraterie betroffene Unternehmen im Maschinen- und Anlagenbau im Jahresvergleich



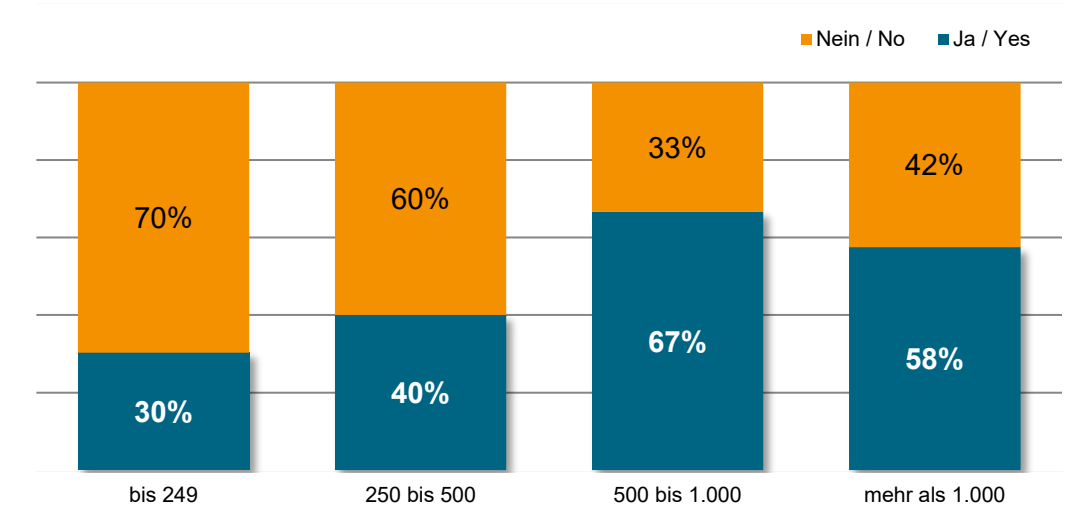
Anteil der betroffenen Unternehmen im Vergleich zu den Vorjahren. N=90 (2024)

Im Jahresvergleich zeigt sich der signifikante Rückgang deutlich: **zum ersten Mal seit zehn Jahren unterschreitet die Quote der durch Produkt- und /oder Markenpiraterie betroffenen Unternehmen die Schwelle von 70 Prozent und unterbietet mit dem historischen Tief von 46 Prozent dabei sogar den Wert zu Beginn der Studie im Jahr 2003.**

Entsprechend scheinen sich die Anstrengungen und Aktivitäten gegen Produkt- und Markenpiraterie bemerkbar zu machen, die in der vergangenen Studie deutlich zugenommen hatten. Mit Blick auf die Ergebnisse zur Frage nach der Art der Plagiate zeigt sich aber auch, dass Kategorien in den Fokus rücken, die bisher noch keine große Rolle eingenommen haben. **Sowohl von unternehmerischer als auch von politischer Seite aus dürfen die Aktivitäten daher keinesfalls nachlassen, sondern müssen sich ebenfalls an die neuen Gegebenheiten anpassen.**

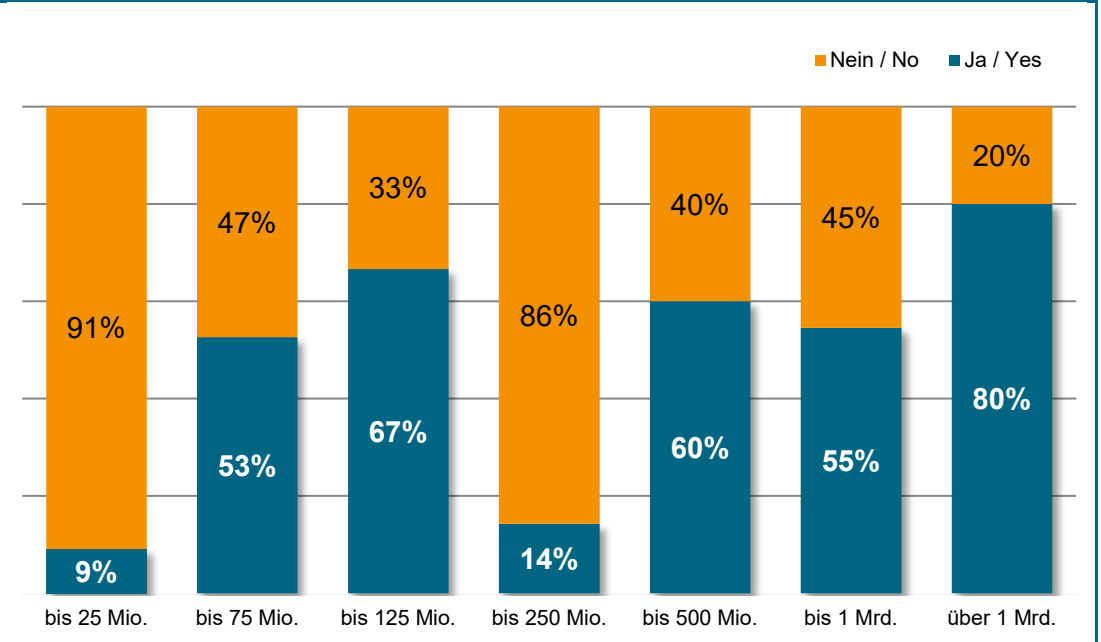
In der Aufschlüsselung der von Produkt- und/oder Markenpiraterie betroffenen Unternehmen nach Unternehmensgröße zeigen sich bekannte Trends. Sowohl nach Mitarbeitendenanzahl als auch nach Jahresumsatz aufgeschlüsselt, steigt mit der Unternehmensgröße der Anreiz für Plagiatoren an diesem Erfolg teilzuhaben.
Der allgemeine Rückgang der Betroffenheit spiegelt sich hier jedoch ebenfalls wider, so dass über alle Unternehmensgrößen hinweg ein niedrigerer Anteil der Betroffenheit von Produkt- und/oder Markenpiraterie zurückgemeldet wurde.

Betroffene Unternehmen nach Unternehmensgröße (Mitarbeitendenzahl)



Anteil der von Produkt- und Markenpiraterie betroffenen Firmen nach Mitarbeitendenzahl. N=90

Betroffene Unternehmen nach jährlicher Umsatzhöhe in EUR



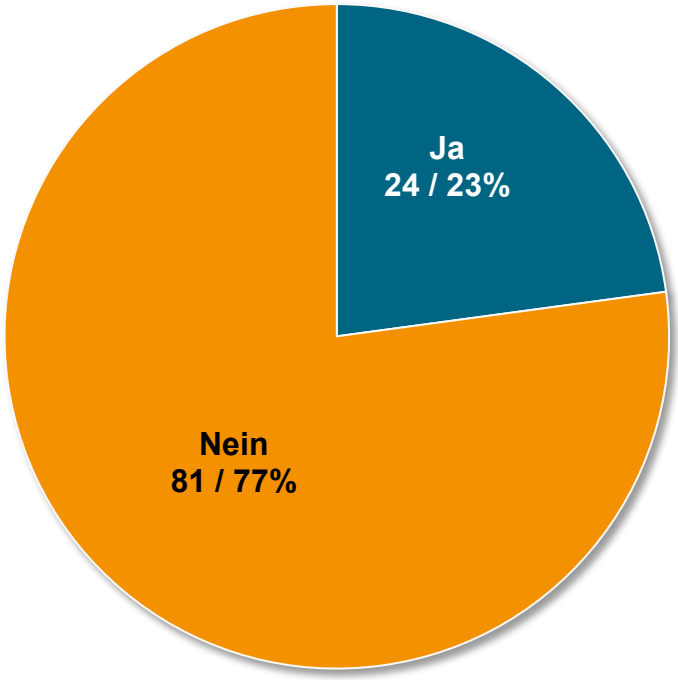
Anteil der von Produkt- und Markenpiraterie betroffenen Unternehmen nach jährlicher Umsatzhöhe in Euro. N=90

4 Betroffenheit in der Industrial Security

Dieses Jahr wurden in die Studie erstmals Fragen aus dem Themenbereich Industrial Security aufgenommen. Auch wenn dieser Themenbereich auf den ersten Blick von klassischer Produkt- und Markenpiraterie losgelöst erscheint, sind die beiden Themen dennoch miteinander verflochten. So können Cybersecurity-Vorfälle in eine destruktive Richtung zielen, beispielsweise mit dem Befall von Ransomware, oder aber in Richtung Industriespionage gehen und damit zum Abfluss von Know-How führen.

Die Frage, ob es im Unternehmen in den vergangenen beiden Jahren zu einem **signifikanten Cybersecurity-Vorfall** gekommen ist, haben **rund eines von vier der befragten Unternehmen bejaht**.

Hatten Sie einen signifikanten Security-Vorfall in ihrem Unternehmen?



Anteil der Unternehmen, die in den vergangenen beiden Jahren einen signifikanten Cybersicherheitsvorfall hatten. N=105

Definition signifikanter Cybersicherheitsvorfall, gem. Art. 23, Absatz 3 der NIS2-Richtlinie:

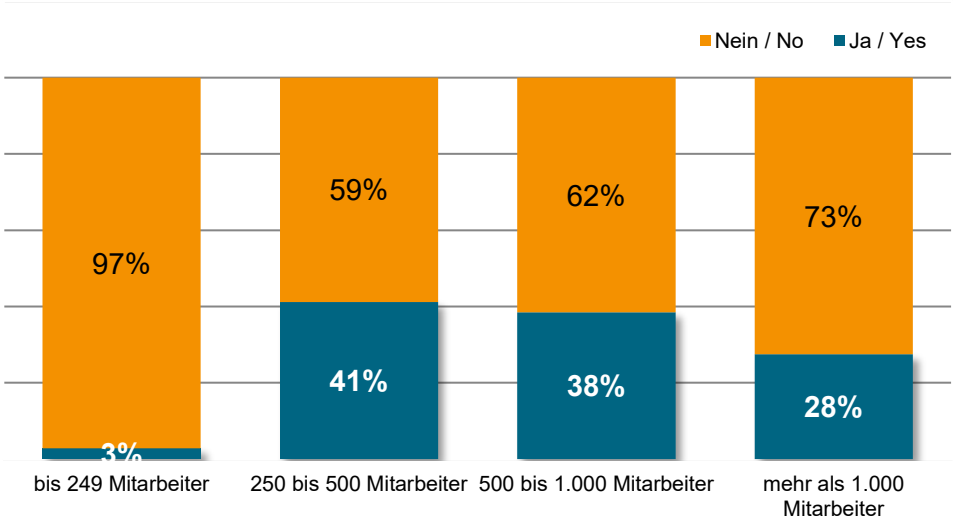
Ein Sicherheitsvorfall gilt als erheblich, wenn

a) er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;
b) er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Aufgeschlüsselt nach Unternehmensgröße zeigt sich bei der Frage nach einem signifikanten Cybersecurity-Vorfall ein ähnliches Bild wie bei der Frage nach Betroffenheit von Produkt- und/oder Markenpiraterie.

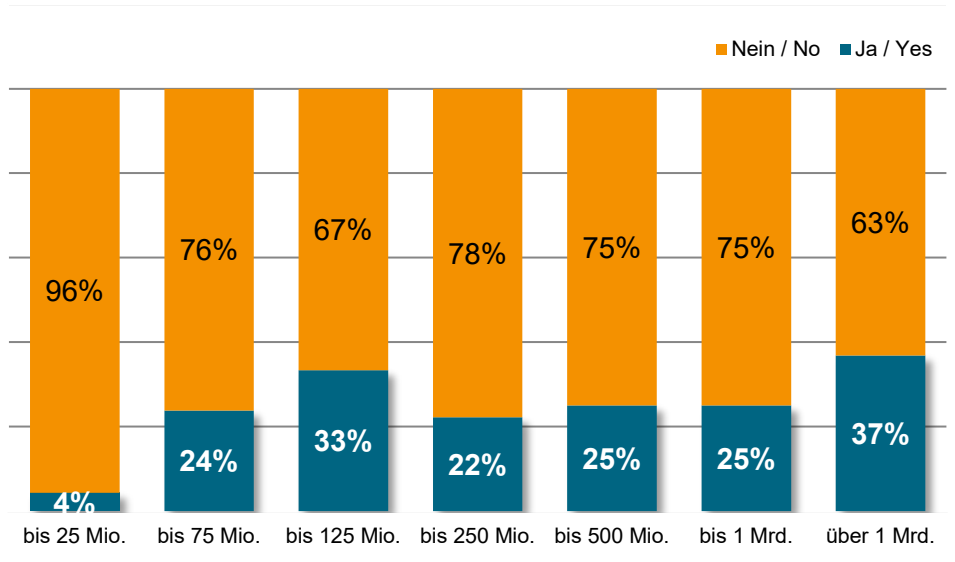
Während kleine Unternehmen mit weniger als 250 Mitarbeitenden beziehungsweise unter 25 Millionen Euro Jahresumsatz über beinahe keine signifikanten Vorfälle berichten, steigt mit der Unternehmensgröße sowohl die Angriffsoberfläche als auch die Attraktivität für Angreifer, so dass im Schnitt eher eines von drei befragten Unternehmen einen signifikanten Cybersecurity-Vorfall vermeldet.

Signifikante Cybersecurity-Vorfälle nach Unternehmensgröße (Mitarbeitendenzahl)



Anteil der Unternehmen mit mindestens einem signifikanten Cybersecurity-Vorfall nach Mitarbeitendenzahl. N=105

Signifikante Cybersecurity-Vorfälle nach jährlicher Umsatzhöhe in EUR

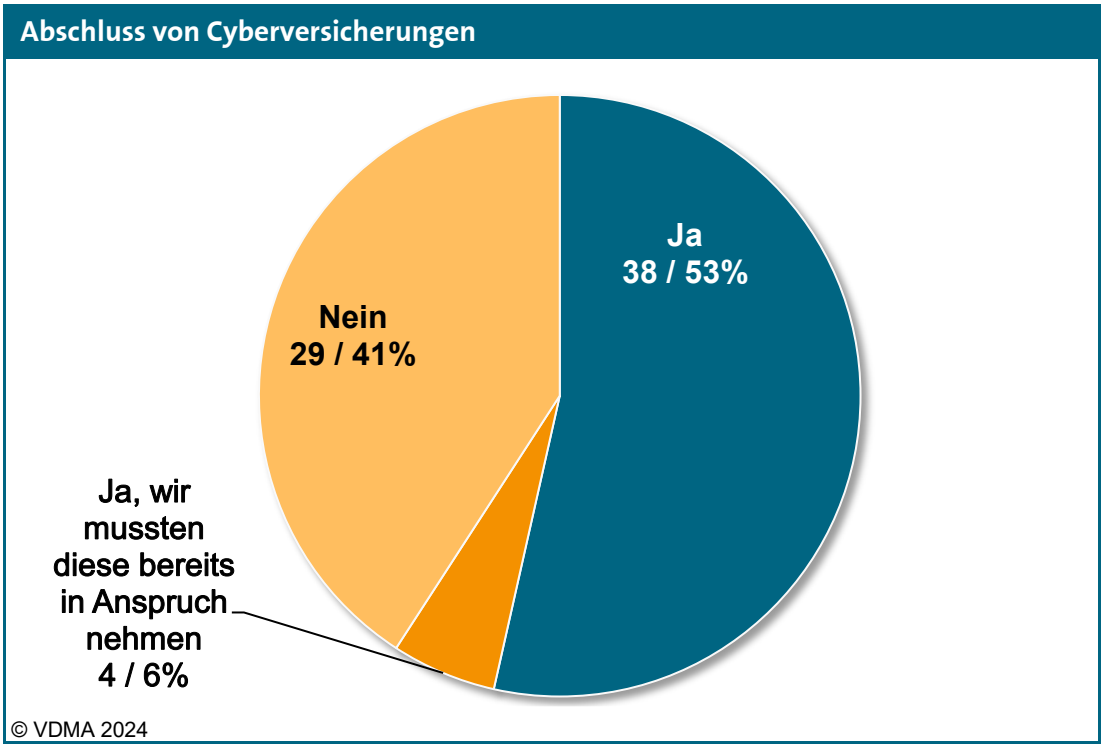


Anteil der Unternehmen mit mindestens einem signifikanten Cybersecurity-Vorfall nach jährlichem Umsatz. N=105

Schäden durch Cybersecurity-Vorfälle können zum Teil nur schwer vorhergesagt beziehungsweise beziffert werden. Aus diesem Grund gibt es sogenannte Cyberversicherungen, mit denen derartige Konsequenzen kontrolliert und reguliert werden können.

Unsere Frage, ob vom Unternehmen Cyberversicherungen abgeschlossen wurden, haben mehr als die Hälfte der Befragten (59 Prozent) bejaht. **In 6 Prozent der Fälle musste diese Cyberversicherung auch bereits in Anspruch genommen werden.** Keiner der Befragten hatte zu einem früheren Zeitpunkt bereits eine Cyberversicherung, diese aber wieder aufgekündigt.

Abschluss von Cyberversicherungen



Vorhandensein und Inanspruchnahme von Cyberversicherungen. N=71

Die VSMA, der Versicherungsmakler des VDMA, berichtet aus den Erfahrungen bezüglich Cyberversicherungen im Maschinen- und Anlagenbau mit seiner „VSMA Marktprognose 2024“ folgendes[1]:
„Die stetig steigenden Risiken wirken sich weiterhin negativ auf den Cyberversicherungsmarkt aus. Die bereits im letzten Jahr zu beobachtende restriktive Zeichnungspolitik der Versicherer setzt sich fort.

Aktuell ist eine Angleichung der Prämien und Selbstbehalte auf ein höheres Marktniveau zu beobachten, von bis zu 30 Prozent über den gesamten Markt gesehen, bei schadensbelasteten Risiken sind auch 150 Prozent Steigerung möglich.

Um bestehende Cyberversicherungen zu verlängern oder neu abzuschließen, müssen Mindeststandards im Bereich der IT-Sicherheit erfüllt werden. Der IT-/Cybersecurity-Reifegrad ist für viele Versicherer entscheidend und wird zum Teil umfassend überprüft.“

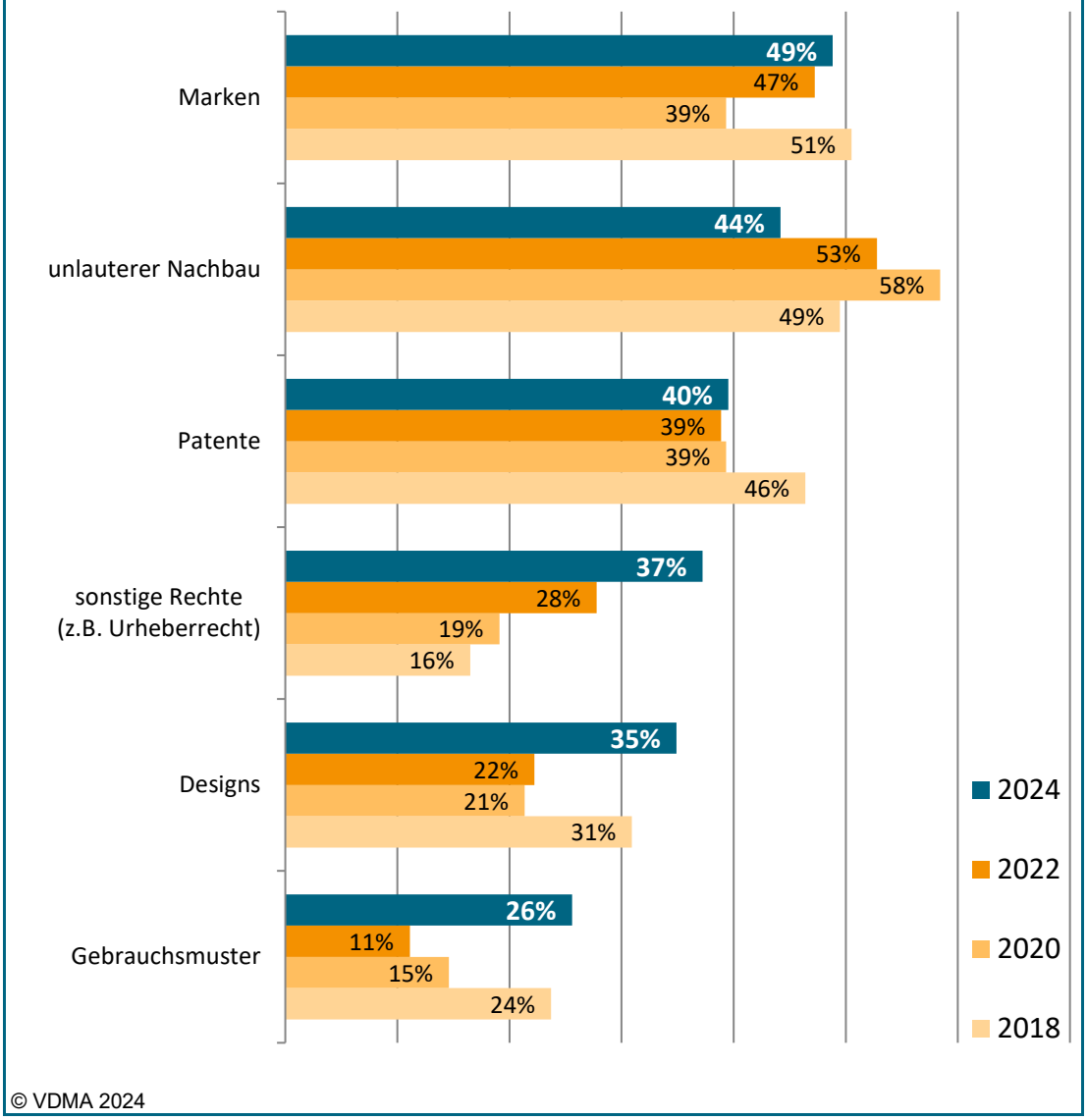
1 https://www.vsma.de/bestellung-vsma-marktprognose/

5 Verletzung von Schutzrechten

Auf die Frage nach der Art der Verletzung von Schutzrechten zeigt sich im Vergleich zur letzten Studie weiterhin ein steter Rückgang des „klassischen“ unlauteren Nachbaus um 9 Prozentpunkte auf nunmehr 43 Prozent.
Mit erneut leichtem Zugewinn ist damit **nun die Markenpiraterie in rund der Hälfte der gemeldeten Fälle auf Platz eins der Schutzrechtsverletzungen.**

Während sich bei Verletzungen des Patentrechts im Vergleich zur letzten Studie keine signifikanten Änderungen ergeben haben, **verzeichnen die Verletzungen von sonstigen Rechten, von Designs und von Gebrauchsmustern ein deutliches Plus.** Die beiden ersten Fälle schlagen damit in mehr als einem von drei Fällen zu Buche. Gerade bei der Schutzrechtsverletzung von Gebrauchsmustern zeigt sich mit einer deutlichen Steigerung auf nun einen von vier Fällen darüber hinaus eine Trendumkehr.

Arten der Schutzrechtsverletzungen durch Produkt- und Markenpiraterie



Arten der Schutzrechtsverletzungen. N=43 (2024, Mehrfachnennungen möglich)

6 Typische Plagiatsarten

Dass hinter einem Plagiat viele verschiedene Formen des Nachahmens und Fälschens stecken können, zeigt sich dieses Jahr erneut in den Antworten auf die Frage nach der Plagiatsart.

Nach einem Rückgang um 7 Prozentpunkte liegen Plagiate des äußeren Erscheinungsbildes mit 56 Prozent nun nur noch auf Platz zwei der typischen Plagiatsarten. **Spitzenreiter sind mit 58 Prozent erneut Plagiate von Komponenten.**

Nachdem sich in der letzten Studie ein Rückgang bei Plagiaten von Katalogen, Broschüren und Produktfotos gezeigt hatte, können sich diese Plagiate mit einem Plus auf 36 Prozent weiterhin auf Platz drei der typischen Plagiatsarten halten.

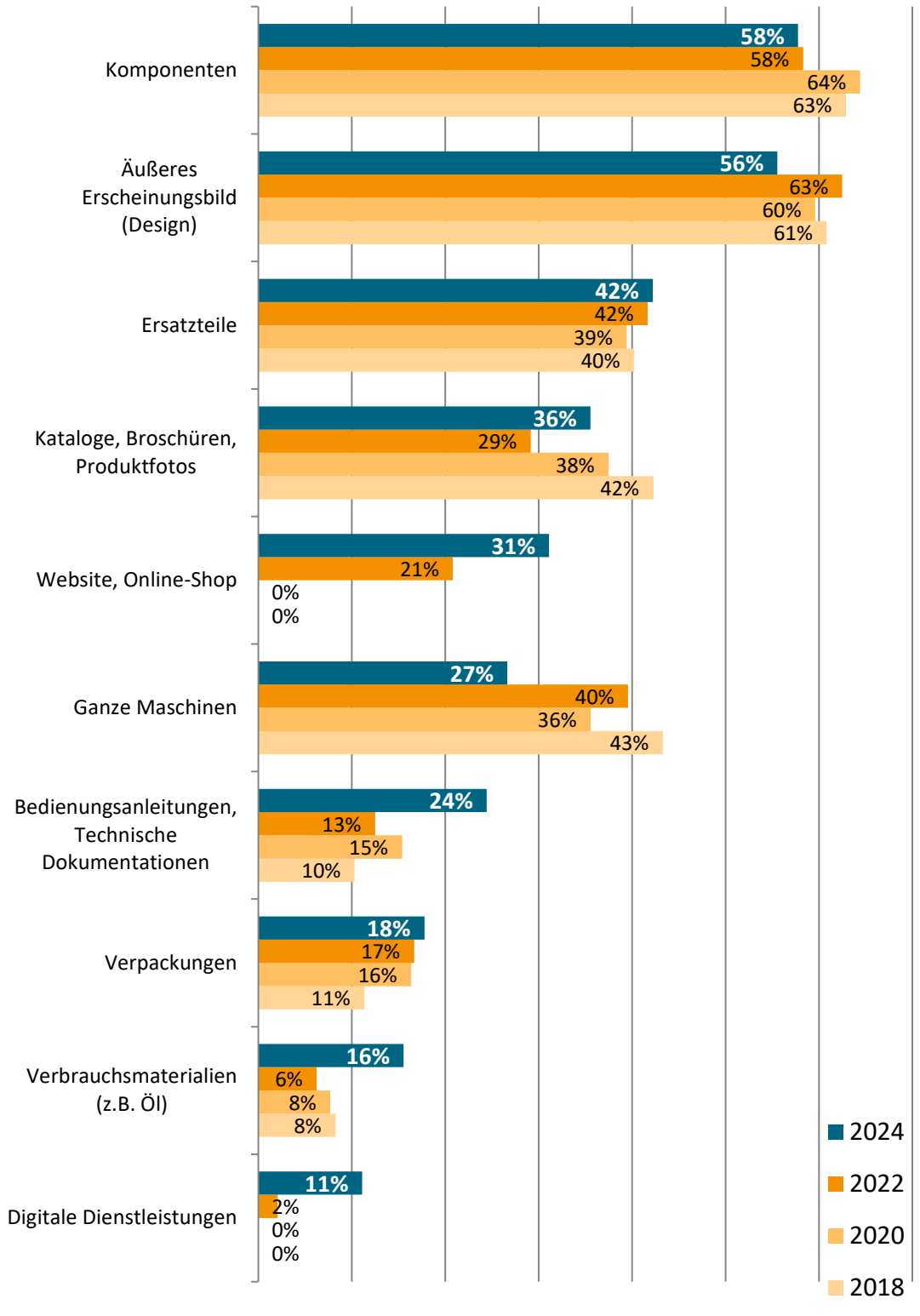
In der letzten Studie wurde erstmals nach Plagiaten von Websites und Online-Shops gefragt, wovon aus dem Stand eines von fünf Unternehmen berichtete. Dieser Wert hat sich um 10 Prozentpunkte auf beinahe eines von drei Unternehmen deutlich erhöht. **Ein ähnlicher Trend zeigt sich bei Plagiaten von digitalen Dienstleistungen, die im Vergleich zur letzten Studie von fünfmal so vielen Unternehmen beobachtet wurden und damit mit 11 Prozent in Erscheinung treten.**

Von einem der letzten Plätze ins Mittelfeld gerutscht sind **Plagiate von Bedienungsanleitungen und technischen Dokumentationen, die von rund einem von vier Unternehmen gemeldet wurden.**

Der einzige signifikante Rückgang ist beim Plagiieren ganzer Maschinen zu verzeichnen. Nach 40 Prozent in der letzten Studie, konnte dieser Plagiatstyp nur noch von etwas mehr als einem von vier Unternehmen beobachtet werden.

Keine signifikanten Änderungen haben sich bei Plagiaten von Komponenten, Ersatzteilen und Verpackungen ergeben.

Was wurde plagiiert?



Arten der Plagiate. N=45 (2024, Mehrfachnennungen möglich)

7 Plagiatoren und deren Auftraggeber

Eine Frage der Studie zielte darauf ab, festzustellen, von wem die Plagiate hergestellt und in Umlauf gebracht werden beziehungsweise wer dies beauftragt.

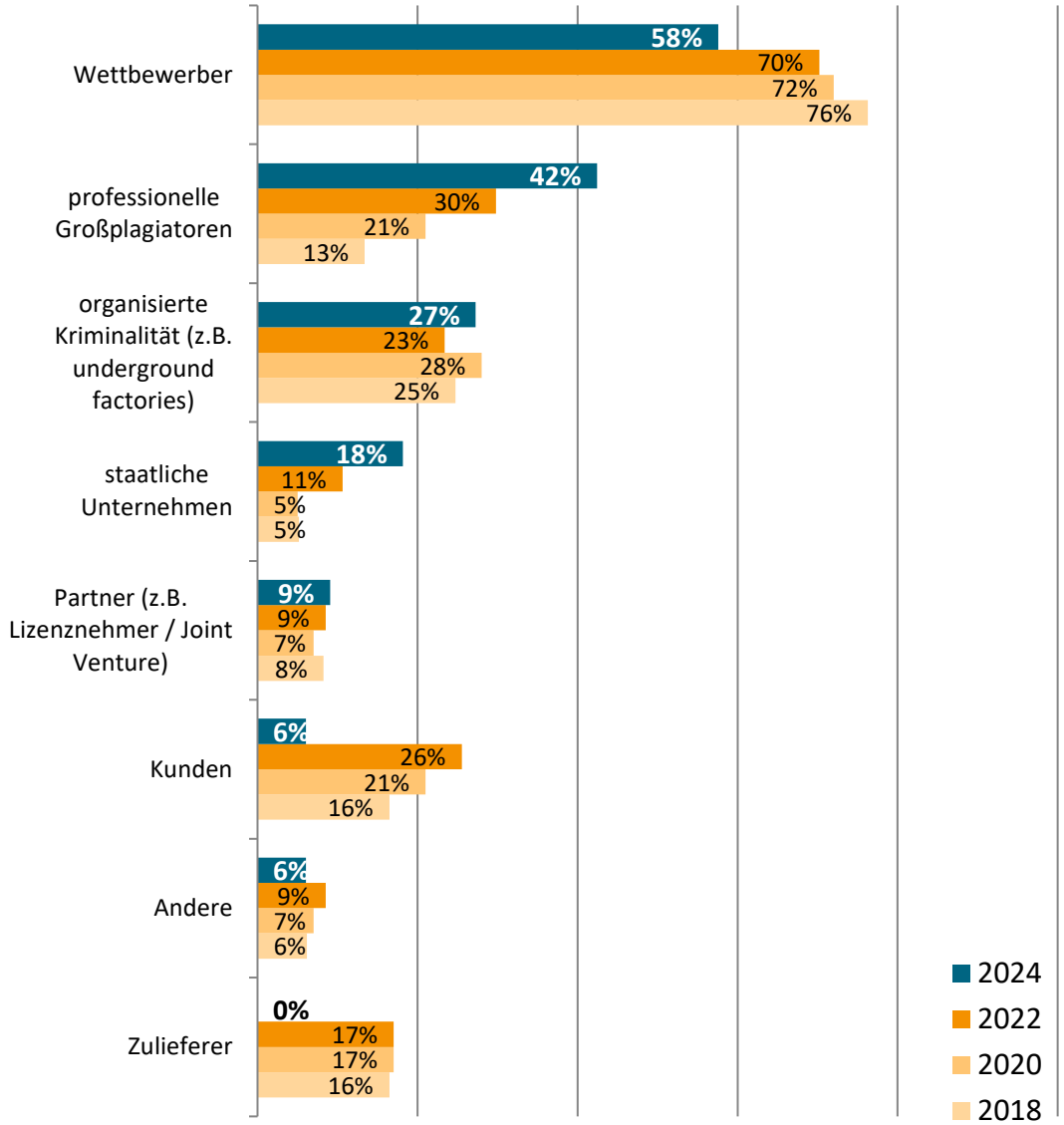
Weiterhin auf Platz eins der Plagiatoren verbleiben direkte Wettbewerber. Mit einem deutlichen Rückgang treten sie jedoch nur noch bei 58 Prozent der Unternehmen in Erscheinung. **Deutlich an Bedeutung gewonnen haben dagegen professionelle Großplagiatoren**, die von 42 Prozent der betroffenen Unternehmen als Urheber von Plagiaten genannt wurden und damit den deutlichen Wachstumstrend seit sechs Jahren fortsetzen.

Ein vergleichbarer Trend zeigt sich bei staatlichen Unternehmen, die mit nunmehr 18 Prozent stetig weiter ins Geschehen rücken.

Während sich bei organisierter Kriminalität und bei direkten Geschäftspartnern keine signifikanten Änderungen zeigen, gibt es beachtliche Rückgänge in der Kategorie von Kunden und Zulieferern: **keines der betroffenen Unternehmen meldete Zulieferer als Quelle von Plagiaten,** und mit einem Rückgang um 77 Prozent **auch nur noch 6 Prozent direkte Kunden.**

Möglicherweise machen sich hier Investitionen in Schutzmaßnahmen für Betriebs- und Geschäftsgeheimnisse bezahlt. Ein Umgehen dieser Schutzmaßnahmen erfordert in der Regel viel Einsatz, der in erster Linie nur von professionellen Großplagiatoren, organisierter Kriminalität oder staatlichen Unternehmen aufgebracht werden kann.

Plagiator, gegebenenfalls Auftraggeber von Plagiaten



Plagiatoren und gegebenenfalls deren Auftraggeber. N=33 (2024, Mehrfachnennungen möglich)

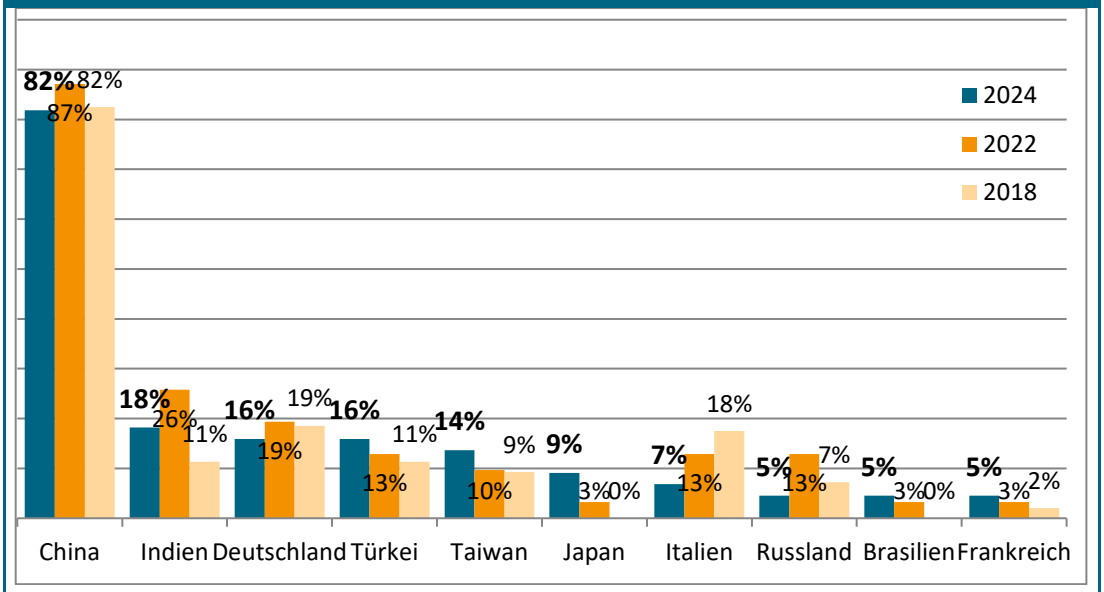
8 Herkunft von Plagiaten

Der unangefochtene Platzhirsch bei der Herkunft von Plagiaten ist und bleibt die Volksrepublik China: **mit leichtem Rückgang nennen 82 Prozent der befragten Unternehmen China als Herstellungsland von Plagiaten.**

Trotz eines Rückgangs auf 18 Prozent folgt **auf Platz zwei Indien**, das erstmals in der vergangenen Studie Deutschland auf Platz drei (diesmal 16 Prozent) verdrängt hatte.

Die Werte von 2020 fehlen in der Betrachtung, da in dieser Studie nur nach dem Vertriebs- nicht jedoch nach dem Herkunftsland von Plagiaten gefragt wurde.

Herkunft der Plagiate



Herkunftsländer, TOP 10 Nennungen N=44 (2024, Mehrfachnennungen möglich)

9 Gefahren durch Plagiate

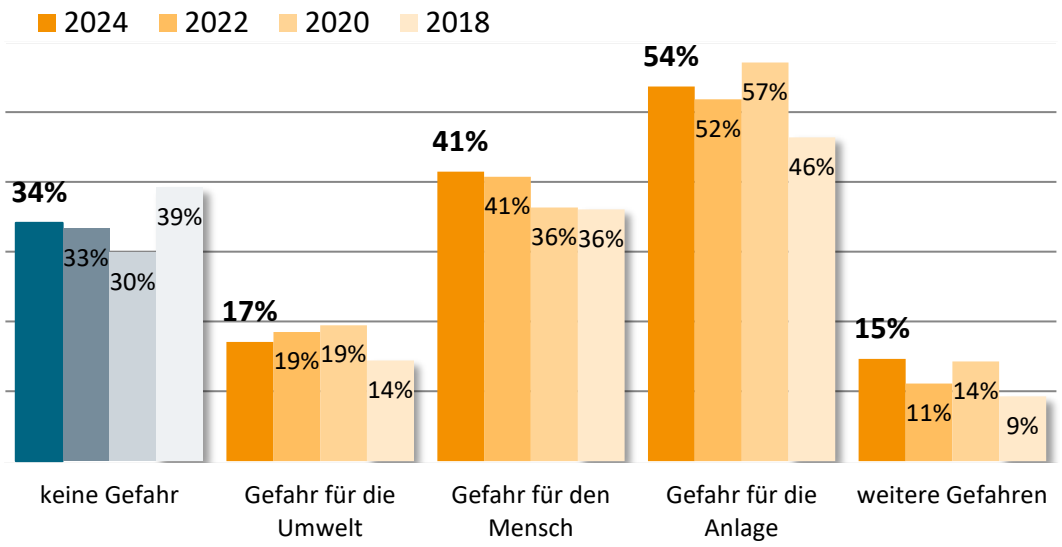
Seit der Studie im Jahr 2016 fragen wir nach potenziellen Gefahren, die die entdeckten Plagiate mit sich bringen, beispielsweise für den Menschen aufgrund fehlender oder funktionsloser Safety-Ausstattungen oder für die Anlage aufgrund qualitativ minderwertiger Ersatzteile.

Dieses Jahr ergaben sich hier keine signifikanten Änderungen: **in mehr als der Hälfte der Fälle entsteht durch die Verwendung eines Plagiats eine Gefahr für die Anlage**, beispielsweise durch höheren Verschleiß beim Verbau qualitativ minderwertiger Ersatzteile. **In mehr als 40 Prozent der Fälle besteht darüber hinaus eine direkte Personengefährdung**, beispielsweise für den Bediener der Maschine.

Lediglich in rund einem von drei Fällen geht von dem Plagiat keine besondere Gefahr aus.

Vereinzelt sahen die Originalhersteller auch Gefahren für das eigene Unternehmen, beispielsweise durch Rufschädigung aufgrund reduzierter Zuverlässigkeit oder geringerer Qualität bei Plagiaten, Wettbewerbsnachteilen oder allgemein wirtschaftliche Einbußen.

Welche Gefahr geht durch die entdeckten Plagiate aus?



Gefährdungspotential entdeckter Plagiate. N=27 (2024, Mehrfachnennungen möglich)

Es sollte daher schon allein im Sinne des sicheren und zuverlässigen Betriebs von Maschinen und Anlagen immer darauf geachtet werden, dass sich keine Plagiate einschleichen. Insbesondere mit Blick auf den Arbeitsschutz der eigenen Mitarbeitenden, aber ebenso aus finanziellen Gründen, da Ausfälle der Anlage oder Reklamationen von Kunden Folgekosten und Imageschäden verursachen können.

10 Unternehmensschaden durch Plagiate

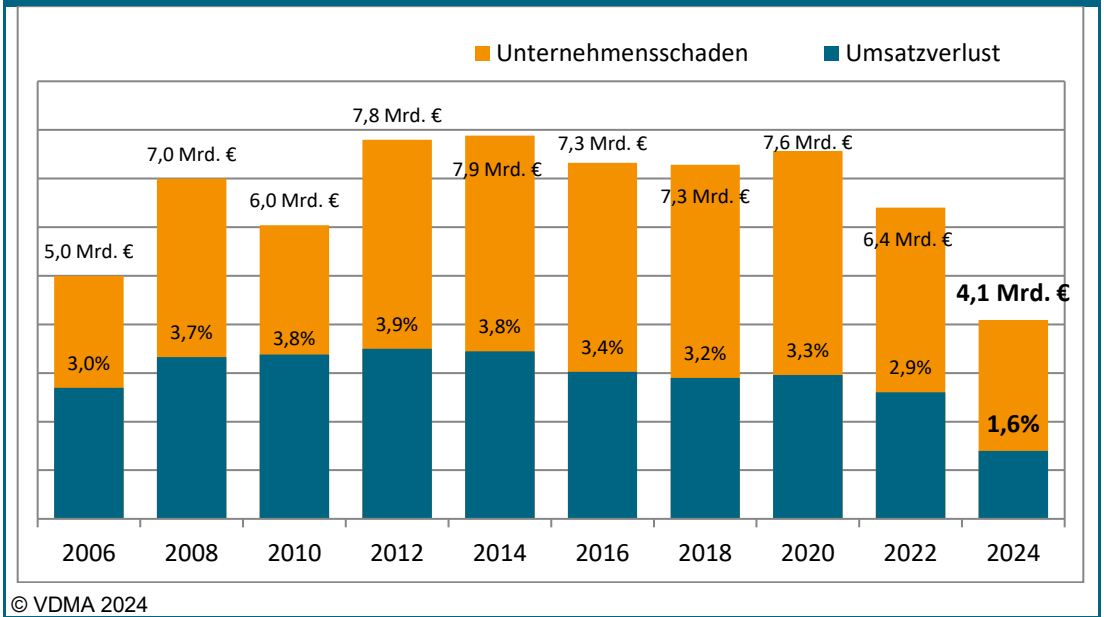
In diesem Kapitel behandeln wir die Frage nach dem geschätzten Unternehmensschaden durch Produkt- und Markenpiraterie. Die Selbsteinschätzung des Unternehmensschadens beruht dabei nicht nur auf dem reinen Umsatzverlust, sondern auch auf gegebenenfalls folgenden Imageschäden, fälschlicher Inanspruchnahme von Gewährleistung, Produkthaftung oder ähnlichem und wurde von den Studienteilnehmenden prozentual angegeben.

Zusammen mit den Werten für den Jahresumsatz und die Anzahl der Mitarbeiter des deutschen Maschinen- und Anlagenbaus[2] aus dem vergangenen Jahr lässt sich daraus eine absolute Zahl für den durch Produkt- und Markenpiraterie verschuldeten Unternehmensschaden und die davon repräsentierten Arbeitsplätze errechnen. Die regelmäßige Befragung und Auswertung des VDMA ergibt hierbei eine gute Abschätzung, wie sich der Schaden durch Produktpiraterie in den letzten Jahren entwickelt hat.

Der geschätzte Unternehmensschaden, der deutschen Maschinen- und Anlagenbauern im Jahr 2023 entstand, führt den generellen Abwärtstrend seit dem Jahr 2014 fort, und springt parallel zur deutlichen Abnahme der Betroffenheit auf das Rekordtief von 1,6 Prozent.

Da im gleichen Zeitraum der Jahresumsatz der gesamten Branche einen Anstieg auf 263,7 Milliarden Euro zu verzeichnen hatte, sinkt der absolute Unternehmensschaden etwas schwächer, aber dennoch deutlich auf 4,1 Milliarden Euro. **Ein Umsatzanteil in dieser Höhe entspricht rund 16.000 Arbeitsplätzen im Maschinen- und Anlagenbau.**

Prozentualer Schaden durch Produktpiraterie im Maschinen- und Anlagenbau

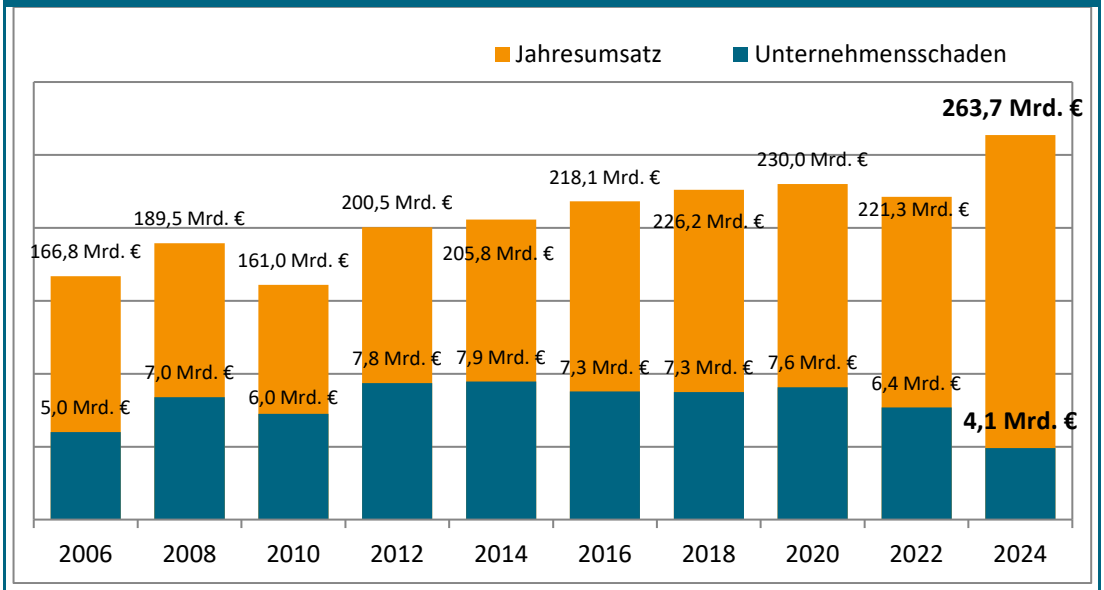


Unternehmensschaden in EUR und Umsatzverlust in Prozent durch Produktpiraterie in Deutschland im Jahresvergleich.

N=47 (2024)

[2] Quelle: Statistisches Bundesamt/VDMA, Betriebe mit mehr als 50 MA.

Absoluter Umsatzschaden durch Produktpiraterie im Maschinen- und Anlagenbau



Branchenumsatz des Vorjahres und Schaden durch Produktpiraterie in Deutschland im Jahresvergleich.

N=47 (2024)

Der Umsatzverlust in Höhe von 1,6 Prozent spiegelt den Gesamtdurchschnitt der Studienteilnehmenden wider. Das heißt, dass nicht nur betroffene Unternehmen inkludiert sind, sondern auch Unternehmen, denen in den vergangenen beiden Jahren kein Schaden entstanden ist.

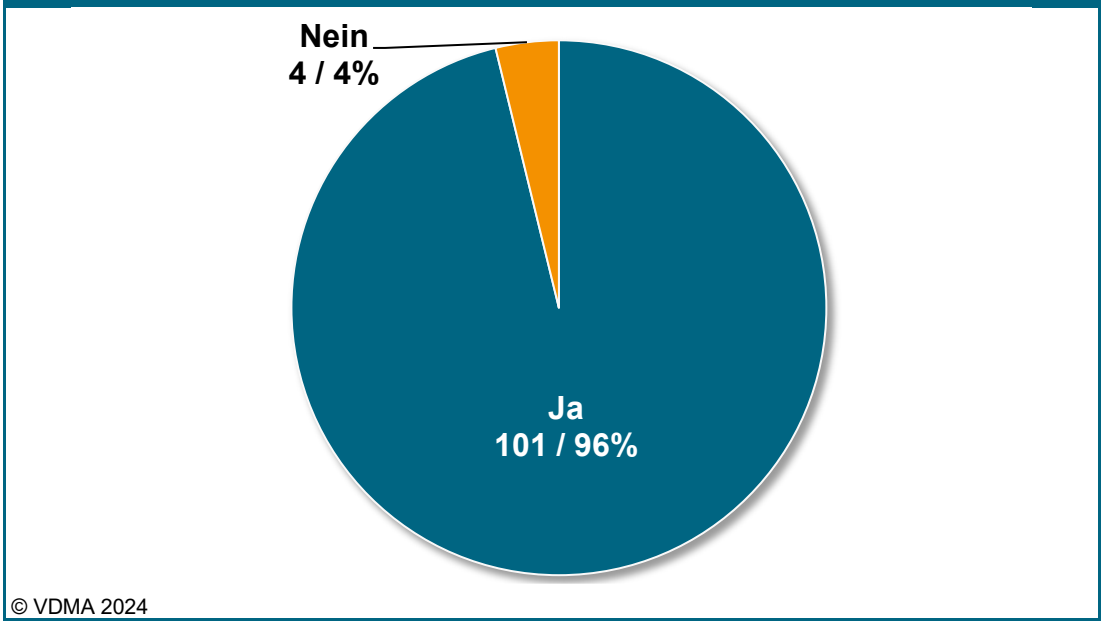
Bezieht man zur Berechnung nur diejenigen Unternehmen ein, die tatsächlich Umsatzverluste durch Produktpiraterie angegeben haben, so stellt sich der durchschnittliche Umsatzverlust naturgemäß höher dar und erreicht im Schnitt einen Wert von 3,5 Prozent.

11 Maßnahmen in der Industrial Security

In Kapitel 4 wurde vorgestellt, wie hoch der Anteil unter den befragten Unternehmen ist, die in den letzten zwei Jahren von einem signifikanten Cybersecurity-Vorfall betroffen waren.

Wir haben nach Cybersecurity-Maßnahmen gefragt, die von den Unternehmen zur Absicherung der Betriebsstätte ergriffen werden. Die eindrucksvolle Zusammenfassung: **96 Prozent der befragten Unternehmen setzen mindestens eine Cybersecurity-Maßnahme um.**

Absicherung der Betriebstätte mit Cybersecurity-Maßnahmen



Anteil der Unternehmen, die mindestens eine Cybersecurity-Maßnahme umsetzen. N=105

Konkret **setzen bereits 95 Prozent der Unternehmen Backup-Maßnahmen ein**, die den Datenverlust von wichtigen Unterlagen, Einstellungsdaten oder Know-How verhindern sollen. **Updates, sowohl für Betriebssysteme als auch für Anwendungssoftware werden ebenfalls von mehr als neun von zehn befragten Unternehmen regelmäßig umgesetzt.**

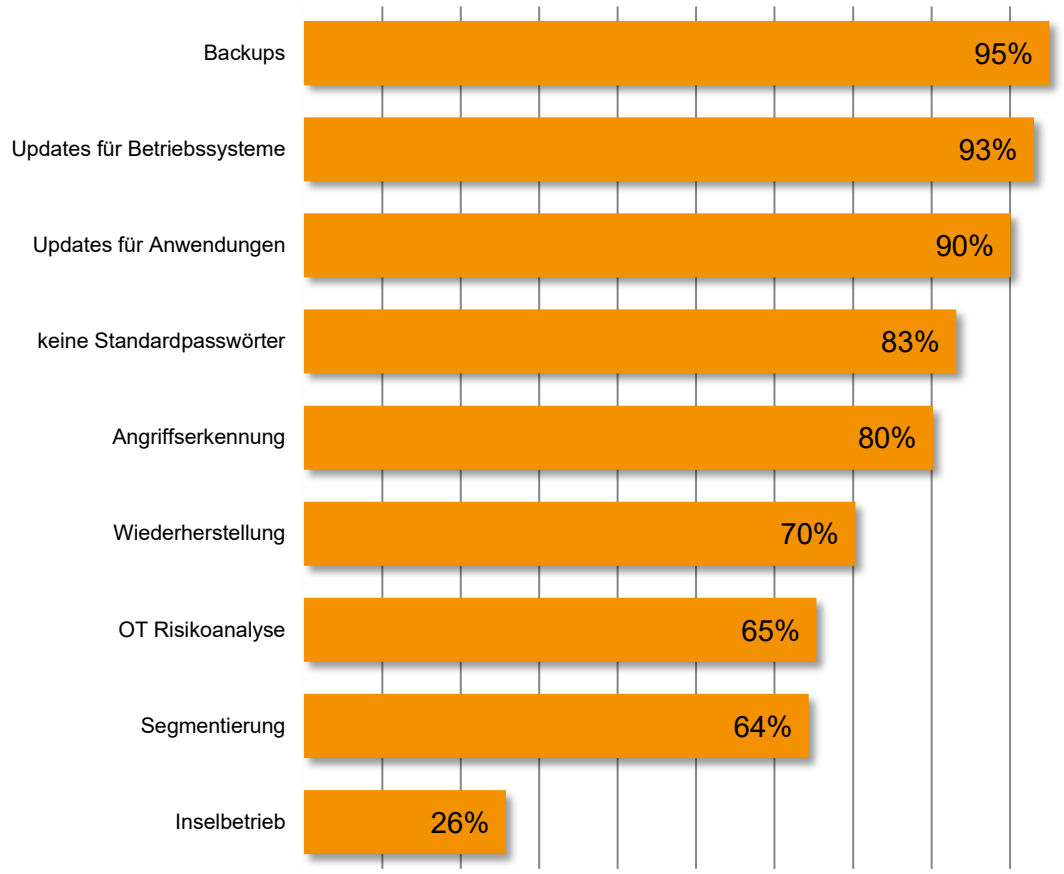
Verwunderlich ist, dass nur 70 Prozent der befragten Unternehmen Wiederherstellung von Daten als Cybersecurity-Maßnahme umsetzen, wobei Backups von 95 Prozent genannt wurden. **Eine Backup-Strategie ohne passende Wiederherstellungs-Prozesse kann sich im Notfall jedoch schnell als unzureichend herausstellen.**

Aktive Angriffserkennung, also die frühzeitige Detektion von Angreifern, um weitere Gegenmaßnahmen einleiten zu können und größere Schäden einzudämmen, wird bei vier von fünf Unternehmen als Maßnahme umgesetzt.

Überraschend ist die Tatsache, dass **nur 83 Prozent der Befragten angeben, keine Standardpasswörter zu verwenden**, sondern ihre Passwörter zu individualisieren. Bildlich gesprochen bedeutet dies im Umkehrschluss, dass bei beinahe einem von fünf Unternehmen der Schlüssel dauerhaft im Türschloss steckt.

Die Cybersecurity-Maßnahme „Inselbetrieb“, die deutlich mehr Eingriff in die Betriebsstätte und Betriebsabläufe bedeutet, dafür aber auch entsprechenden Schutz bieten kann, wird von einem von vier der befragten Unternehmen umgesetzt.

Cybersecurity-Maßnahmen zur Absicherung der Betriebstätte gegen Angriffe



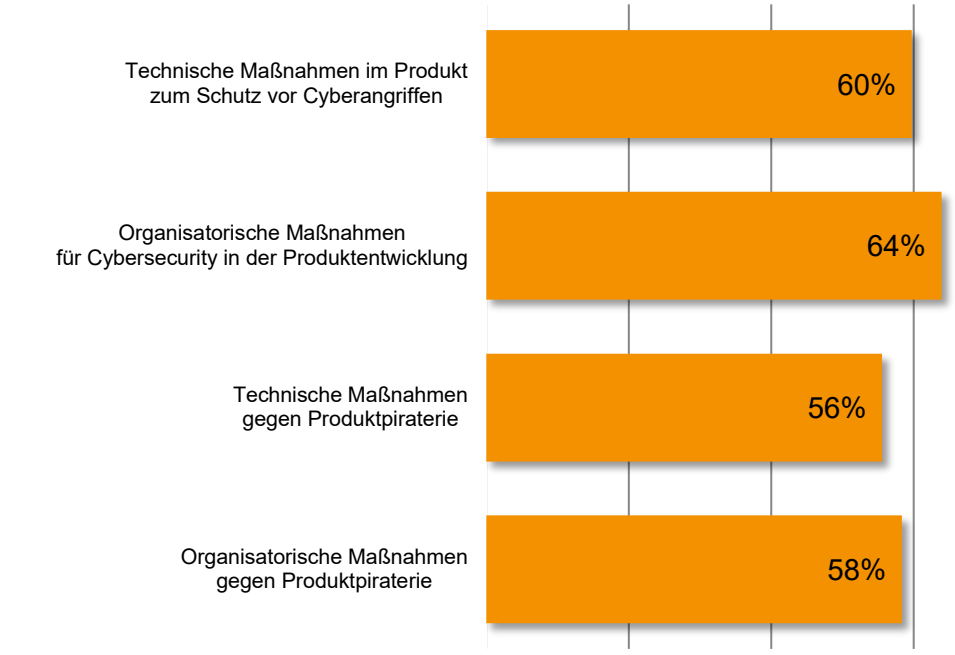
Ergriffene Cybersecurity-Maßnahmen zur Absicherung der Betriebsstätte. N=101

Neben den Maßnahmen zur Absicherung der Betriebsstätte haben wir ebenfalls nach Maßnahmen für Produktsicherheit in der Produktentwicklung gefragt.

Hier zeigt sich zum einen, dass der Schutz vor Cyberangriffen bei den befragten Unternehmen einen geringfügig höheren Stellenwert einnimmt als das Ergreifen von Maßnahmen gegen Produktpiraterie.
Zum anderen zeigt sich, dass organisatorische Maßnahmen in beiden Fällen geringfügig häufiger umgesetzt werden als technische Maßnahmen.

Aufgrund der Stichprobengröße von 72 sind die einzelnen Unterschiede jedoch nicht signifikant. **Dennoch wird deutlich, dass rund drei von fünf Unternehmen Produktschutzmaßnahmen ergreifen.**

Produktschutz-Maßnahmen in der Produktentwicklung



Anteil der Unternehmen, die Produktschutz-Maßnahmen in der Produktentwicklung ergreifen. N=72

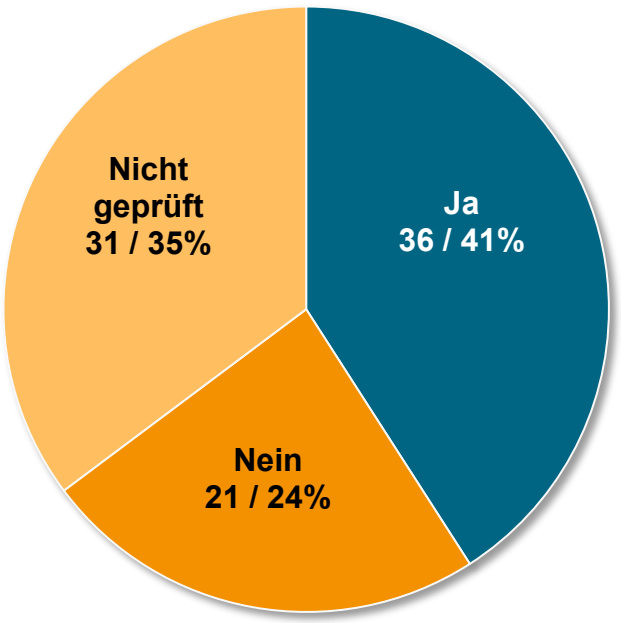
12 NIS2 – Betroffenheit

Die Network and Information Systems Directive 2 (NIS2) ist eine Richtlinie der EU, die zum 16. Januar 2023 in Kraft getreten ist und in den Mitgliedsstaaten in nationale Gesetze umgesetzt werden muss, in Deutschland durch das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG). Die NIS2 weitet den Anwendungsbereich von klassisch kritischer Infrastruktur (KRITIS) auf weitere wichtige Einrichtungen aus. Der Maschinenbau ist im Anwendungsbereich für sonstige kritische Sektoren aufgenommen worden und ist damit direkt von der NIS2 erfasst.
Wir haben daher gefragt, welche unserer Mitgliedsunternehmen in Anwendungsbereich der nationalen NIS2-Umsetzung fallen.

Rund ein Drittel (35 Prozent) der befragten Unternehmen gaben an, noch nicht geprüft zu haben, ob sie in den Anwendungsbereich fallen. **Von denjenigen Unternehmen, die die Prüfung bereits durchgeführt haben, fallen beinahe zwei Drittel (63 Prozent) in den Anwendungsbereich.**

Der VDMA hat die Unternehmen mit negativem Prüfergebnis nochmals selbst analysiert und dabei festgestellt, dass von den 21 Unternehmen lediglich sechs Unternehmen tatsächlich nicht in den Anwendungsbereich der NIS2-Umsetzung fallen.
Die 15 Unternehmen, die sich nicht im Anwendungsbereich der NIS2 sehen, wurden vom VDMA kontaktiert und explizit auf die Betroffenheit hingewiesen. **Unter Berücksichtigung der Gegenprüfung durch den VDMA ergibt sich eine NIS2-Betroffenheit von ca. 90 Prozent**. 71 Prozent der Unternehmen mit einer negativen Prüfung kamen zu einer falschen Einschätzung.

Fallen Sie in den Anwendungsbereich der nationalen NIS2-Umsetzung?



Anwendungsbereich der nationalen NIS2-Umsetzung. N=88

13 Standards in der Industrial Security

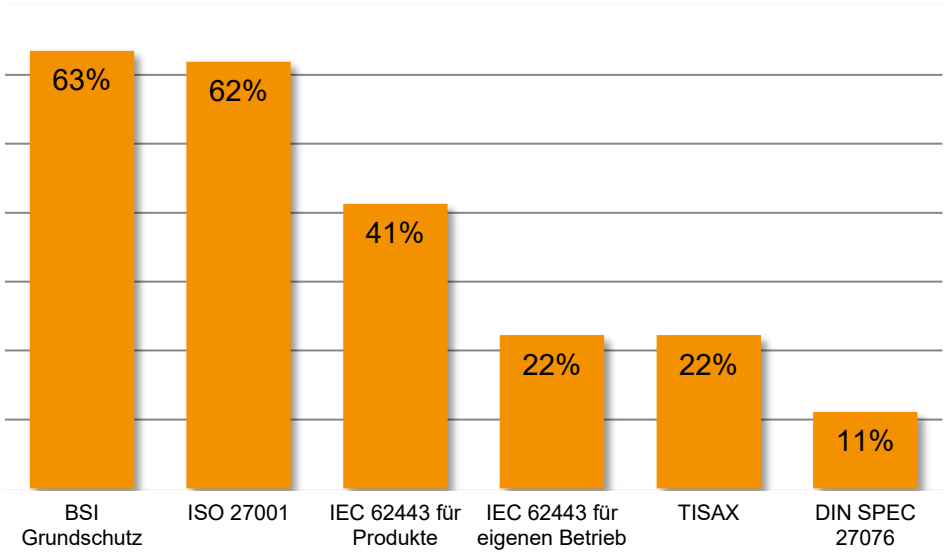
Anforderungen an die Industrial Security kommen nicht nur aus der Politik und der nationalen und internationalen Gesetzeslandschaft, sondern auch aus technischen und organisatorischen Standards, deren Umsetzung teilweise von Kunden oder Geschäftspartnern gefordert wird.

Auf unsere Frage gaben die Unternehmen an, dass der **Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik, sowie der ISO-Standard 27001 die verbreitetsten Standards sind, die beinahe von zwei von drei Unternehmen angewandt werden.**

Mit 41 Prozent folgt dahinter auf Platz drei der Standard IEC 62443, angewandt auf die eigenen Produkte.

IEC 62443, angewandt auf den eigenen Betrieb, sowie TISAX, ein verbreiteter Standard in der Automobilindustrie, werden mit jeweils 22 Prozent von etwas mehr als jedem fünften befragten Unternehmen umgesetzt.

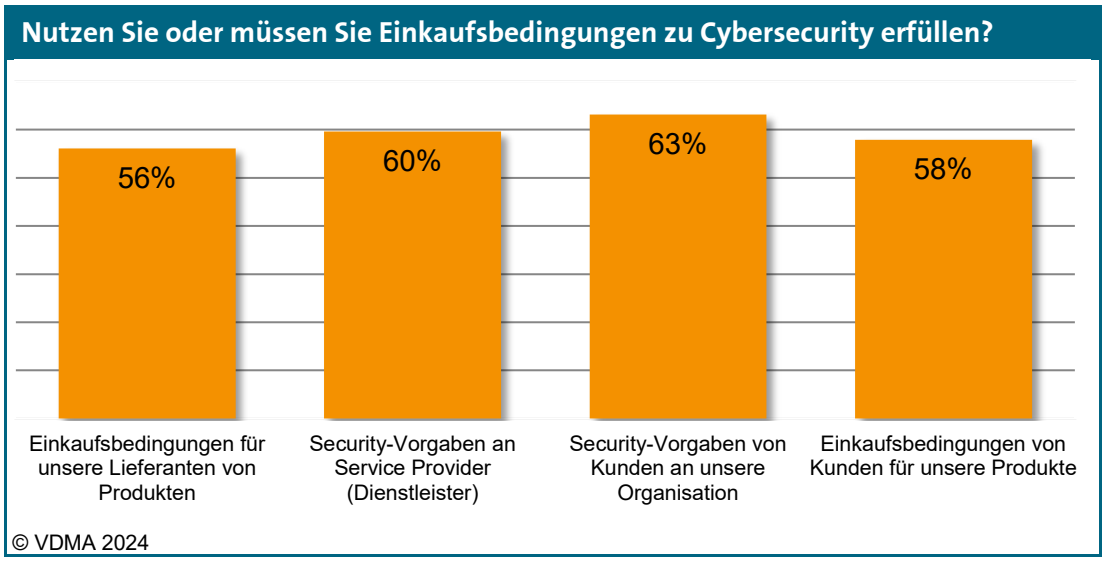
Welche Standards werden von Ihrem Unternehmen angewandt?



Umsetzung von einschlägigen Standards aus dem Bereich Industrial Security. N=63

Dass die Einhaltung von Standards sowohl von Kunden als auch von Geschäftspartnern gefordert wird, zeigen die Rückmeldungen der Unternehmen auf unsere Frage, ob sie Bedingungen und Vorgaben von ihren Lieferanten beziehungsweise Dienstleistern verlangen, oder selbst Vorgaben von Kunden für ihre Organisation oder Produkte bekommen.

In allen Kategorien wurden diese Fragen von rund 60 Prozent der Unternehmen bejaht, was sich gut mit der Umsetzung des BSI-Grundschutz und dem ISO-Standard 27001 deckt.



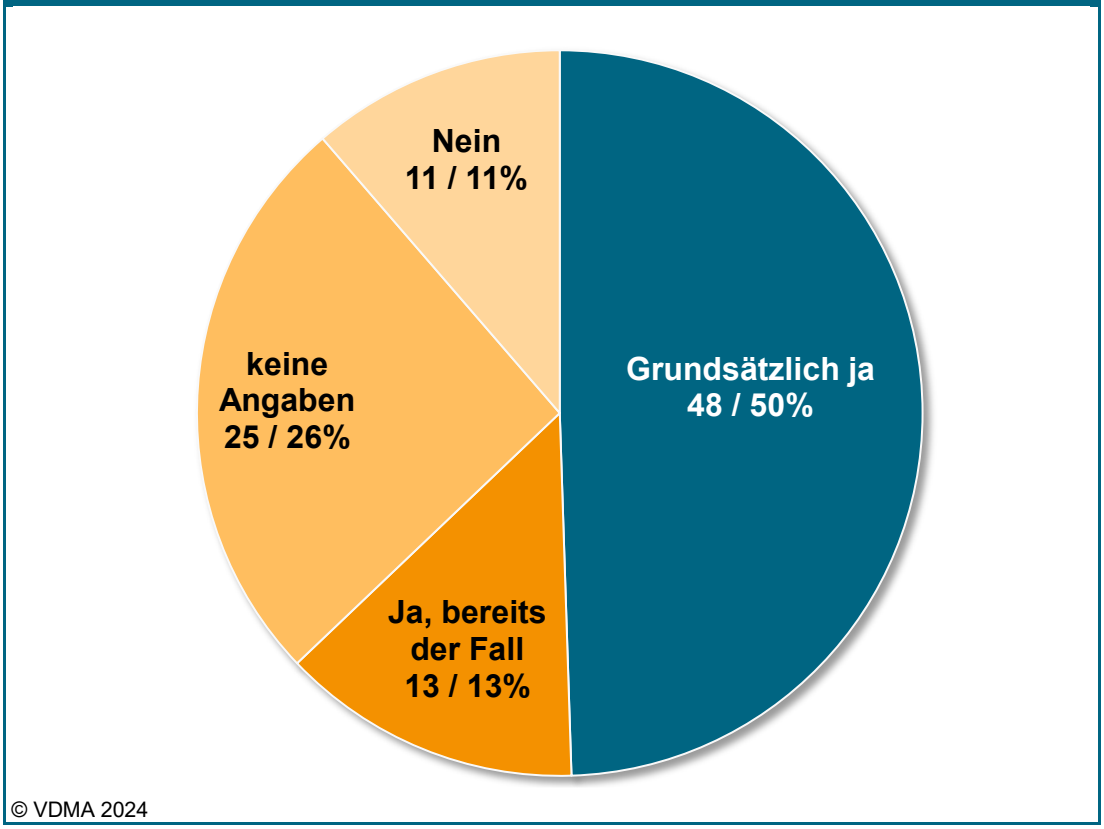
Vorgaben zu Einkaufsbedingungen aus dem Bereich Industrial Security. N=57

14 Bündnis für Cybersecurity

Falls es zu einem Cyberangriff kommt, könnten Unternehmen neben eigenen Kapazitäten oder Dienstleistern auch auf vorab geschlossene Allianzen oder Bündnisse zurückgreifen, beispielsweise um sich gegenseitig mit entsprechend geschultem IT-Personal zu unterstützen.
Im Rahmen der Studie haben wir daher konkret nach der Bereitschaft gefragt, sich in solch einem lokalen oder regionalen Cyberbündnis zu engagieren.

Die überwiegende Mehrheit der befragten Unternehmen wäre dazu entweder grundsätzlich bereit (50 Prozent), beziehungsweise ist bereits in einem Cyberbündnis aktiv (13 Prozent). Im Gegensatz dazu schließt nur eines von zehn Unternehmen ein solches Engagement derzeit aus.

Würden Sie sich in einem Cyberbündnis engagieren?



Stimmungsbild zum Engagement in einem lokalen oder regionalen Cyberbündnis. N=97

15 Der VDMA handelt

Produktpiraterie

Die Aktivitäten des VDMA gegen Produktpiraterie haben sich seit ihrem Start mit dieser Studie im Jahr 2003 kontinuierlich weiterentwickelt. Standen zu Beginn insbesondere die Information und Sensibilisierung von Politik und Gesellschaft im Vordergrund, konzentrieren sich die aktuellen Maßnahmen auf die Verbesserung der Strafverfolgung und den Austausch zwischen betroffenen Unternehmen.

Damit die erforschten Produktschutz-Innovationen maschinenbauspezifisch weiterentwickelt werden, etablierte der VDMA im Jahr 2010 die Arbeitsgemeinschaft Produkt- und Know-how-Schutz (AG Protect-ing). Nach erfolgreicher Arbeit ging die Arbeitsgemeinschaft im Jahr 2016 in den **Arbeitskreis „Gewerblicher Rechtsschutz“** auf.
Der VDMA-Arbeitskreis "Gewerblicher Rechtsschutz" verbindet und informiert interessierte Mitgliedsunternehmen des VDMA über die neusten Entwicklungen des gewerblichen Rechtsschutzes und bietet einen vertraulichen Raum zum Erfahrungsaustausch über rechtliche, technische und organisatorische Aktivitäten.

Industrial Security

Bereits seit 2006 betreut die VDMA Abteilung Informatik das übergreifende Feld der Informationssicherheit. Die Gründung des Arbeitskreises „Informationssicherheit“ im Jahr 2008 bildet noch immer die Basis und wurde im Jahr 2012 durch den Austausch zu Security in Produktion und Automation ergänzt (nun „Industrial Security“).
Neueste Aktivität ist der in 2023 gegründete Arbeitskreis „NIS2“, in dem Klein- und mittelständische Unternehmen gemeinsam Ihr Verständnis zur NIS2-Richtlinie erarbeiten.

Im Jahr 2019 startete der Arbeitskreis „Industrial Security“ die wesentlichen Arbeiten im wichtigen Bereich der „Supply Chain Security“. Die Cybersecurity der Lieferkette funktioniert nur, wenn alle Beteiligten Ihren Beitrag leisten und wenn die Anforderungen und Maßnahmen abgestimmt werden. Dies erfordert eine verbandsübergreifende Zusammenarbeit mit dem BSI, den Zulieferern im ZVEI und bitkom sowie mit den Kundengruppen.

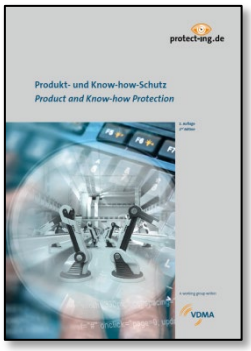
Erfolgreiches Abbild der Zusammenarbeit in den VDMA-Arbeitskreisen sind die standardisierten Fragebögen für die konkrete Beschaffung von Maschinen, ein allgemeiner Lieferantenfragebogen, oder auch das Mapping von ISO27001 zur NIS2.

Rechtliche Schutzmaßnahmen

Der rechtliche Schutz bildet für die meisten Unternehmen die Basis im Kampf gegen Produktpiraterie. Wir informieren unsere Mitgliedsunternehmen in Broschüren und Vorträgen über rechtliche Möglichkeiten zum Innovationsschutz und stellen Vertragsmuster zur Verfügung. In persönlichen Gesprächen erörtern wir Problemfälle und helfen bei der Anmeldung von Schutzrechten und vertraglichen Formulierungen.

Unsere Kooperationen mit Kanzleien in den wichtigsten ausländischen Märkten ermöglichen eine schnelle und kompetente Beratung vor Ort.

16 Publikationen des VDMA zu Produktpiraterie



Branchenführer "Produkt- und Know-how-Schutz"

Sprache: Deutsch und Englisch
Preis: kostenfrei

Beiträge zu Produktpiraterie, Security und Know-how-Schutz. Übersicht von Technologien, Schutzmaßnahmen und Lösungen in der (aufgelösten) Arbeitsgemeinschaft inkl. Matrix.

Auf Anfrage bei Biljana Gabric erhältlich: biljana.gabric@vdma.org

Leitfaden "Produkt- und Know-how-Schutz"

Sprache: Deutsch oder Englisch
Preis: kostenfrei nach Registrierung als PDF

Anleitung zum erfolgreichen Einsatz von Schutzmaßnahmen inkl. praxisnaher Beispiele.

Auf Anfrage bei Biljana Gabric erhältlich: biljana.gabric@vdma.org

INS-Studie "Integratives System zur einheitlichen Kennzeichnung und Identifizierung von Maschinenbauprodukten"

Sprache: Deutsch
Preis: kostenfrei als PDF

Übersicht über Kennzeichnungstechnologien und deren Eignung für verschiedene Einsatzzwecke.

Auf Anfrage bei Biljana Gabric erhältlich: biljana.gabric@vdma.org

Piraterierobuste Gestaltung von Produkten und Prozessen
ISBN 978-3-8163-0601-6

Band 1 der Reihe „Innovationen gegen Produktpiraterie“ mit Ergebnissen aus den Projekten:

- PiratPro
- Protactive
- ProProtect

https://www.vdmashop.de/Informatik-und-Technik/Piraterierobuste-Gestaltung-von-Produkten-und-Prozessen.html

Kennzeichnungstechnologien zum wirksamen Schutz gegen Produktpiraterie
ISBN 978-3-8163-0602-3

Band 2 der Reihe „Innovationen gegen Produktpiraterie“ mit Ergebnissen aus den Projekten:

- O-Pur
- EZ-Pharm
- Mobil Authent

https://www.vdmashop.de/Informatik-und-Technik/Kennzeichnungstechnologien-zum-wirksamen-Schutz-gegen-Produktpiraterie.html

Wirksamer Schutz gegen Produktpiraterie im Unternehmen
ISBN 978-3-8163-0603-0

Band 3 der Reihe Innovationen gegen Produktpiraterie mit Ergebnissen aus den Projekten:

- ProOriginal
- KoPira
- KoPiKomp
- ProAuthent

https://www.vdmashop.de/Informatik-und-Technik/Wirksamer-Schutz-gegen-Produktpiraterie-im-Unternehmen.html

17 Publikationen des VDMA zu Industrial Security

VDMA Lieferantenselbstauskunft (Excel)

Sprache: Deutsch, Englisch
Preis: kostenfrei

Allgemein gültiger Fragebogen an Lieferanten ohne konkreten Beschaffungsbezug. Referenz auf Maschinenverordnung und Cyber Resilience Act. Mit dem BSI gemeinsam erarbeitet.

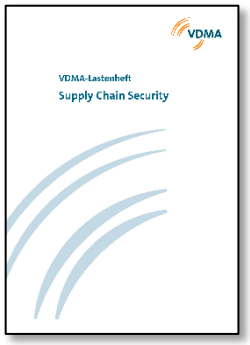
https://www.vdma.org/viewer/-/v2article/render/82349740

VDMA Mapping NIS2-27001:2002 (Excel)

Sprache: Englisch
Preis: kostenfrei, nur für VDMA-Mitglieder

Mapping der ISO/IEC 27001:2022 auf die Anforderungen aus der NIS2-Richtlinie sowie des NIS2UmsuCG (nach dem jeweiligen Sachstand des Referentenentwurfs).

Auf Anfrage erhältlich.

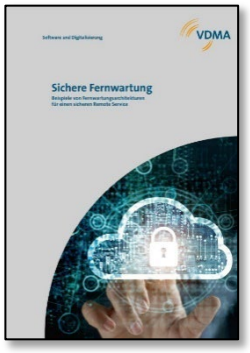


VDMA Lastenheft "Supply Chain Security"

Sprache: Deutsch
Preis: kostenfrei

Lastenheft mit Cybersecurity-Anforderungen auf Basis der IEC 62443. Zielgruppe sind Einkäufer, die allgemein anerkannte Anforderungen an die Cybersecurity von Maschinen und Anlagen stellen möchten, vom Design bis hin zum cybersicheren Betrieb.

https://www.vdma.org/viewer/-/v2article/render/73448513



Sichere Fernwartung im Maschinen- und Anlagenbau

Sprache: Deutsch
Preis: kostenfrei, nur für Mitglieder

Beispiele von Fernwartungsarchitekturen zeigen auf, wie der Maschinen- und Anlagenbau einen sicheren Service aus der Ferne gewährleisten kann.

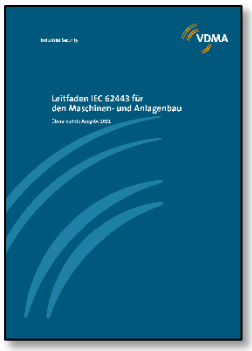
https://www.vdma.org/viewer/-/v2article/render/45231112

Mindestempfehlungen zu Security in der Supply Chain

Sprache: Deutsch
Preis: kostenfrei

Mindestempfehlungen für Maschinen- und Anlagenbauer zu technischen, organisatorischen und prozessualen Anforderungen bei der Umsetzung von Security für Produkte und Prozesse.

https://www.vdma.org/viewer/-/v2article/render/51129051

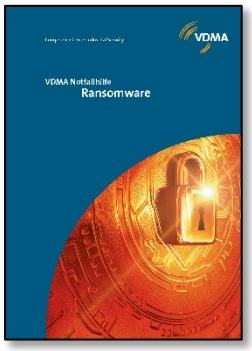


VDMA Leitfaden IEC 62443 für den Maschinen- und Anlagenbau

Sprache: Deutsch, Englisch
Preis: 50 Euro für Nicht-Mitglieder, kostenfrei für Mitglieder

Beschreibung eines Weges durch die IEC 62443, als Integrator einer Maschine nach Security-Level 2, inkl. Beispielen nach 62443-3-3.

https://www.vdma.org/viewer/-/v2article/render/16110956



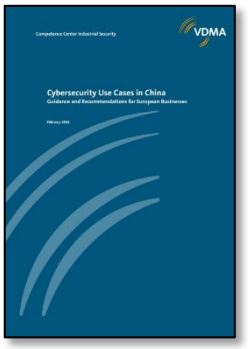
VDMA Notfallhilfe Ransomware

Sprache: Deutsch
Preis: kostenfrei

Unterstützung, Handlungsempfehlung bei einer Infektion mit Ransomware, Kontaktstellen bei Behörden und Dienstleistern. Liste von Indikatoren für eine Infektion und Maßnahmen.

https://industrialsecurity.vdma.org/viewer/-/v2article/render/47727760

18 Publikationen des VDMA zu Cybersecurity in China



Cybersecurity Use Cases in China – Guidance and Recommendations

Sprache: Englisch
Preis: kostenfrei, nur für Mitglieder

Kleine und mittlere Unternehmen benötigen eine praktische Anleitung für Cybersecurity in China.
In fünf industrienahen Use Cases werden Fragen beantwortet und Empfehlungen ausgesprochen, mit Unterstützung von Sinolytics.

https://www.vdma.org/viewer/-/v2article/render/48588138

Policy Briefing on the Chinese Cross-Border Data Transfer Measures

Sprache: Englisch
Preis: kostenfrei, nur für Mitglieder

Information und Empfehlung von VDMA und Sinolytics zu den Vorgaben für den grenzüberschreitenden Datentransfer von „Important Data“ und „Personal Information“, Stand 03/2023

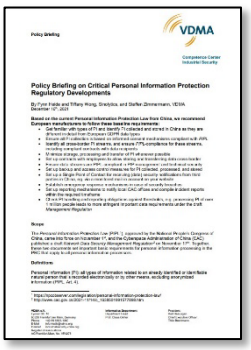
https://www.vdma.org/viewer/-/v2article/render/69389762

Datenschutz: Chinesische Standardvertragsklauseln (C-SCC)

Sprache: Deutsch/Englisch (Artikel)
Preis: kostenfrei, nur für Mitglieder

Information über die von der Cyberspace Administration of China (CAC) veröffentlichten Standardvertragsklauseln (C-SCC) im Rahmen einer Verordnung vom 24. Februar 2023. Die Verordnung trat am 1. Juni 2023 in Kraft.

https://www.vdma.org/viewer/-/v2article/render/76106748

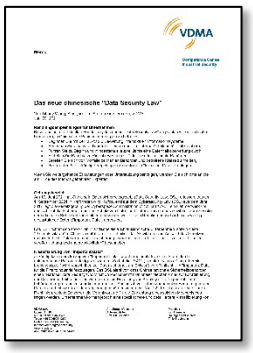


China's Personal Information Processing (PIP) Law

Sprache: Englisch
Preis: kostenfrei, nur für Mitglieder

Informationen und Empfehlung von VDMA und Sinolytics zum Ende 2021 in Kraft getretenen Gesetz zum Umgang und Schutz von personenbezogenen Daten (PIP Law).

https://www.vdma.org/viewer/-/v2article/render/39322985



Das chinesische Data Security Law

Sprache: Deutsch, Englisch
Preis: kostenfrei, nur für Mitglieder

Das Policy Briefing von VDMA und Sinolytics nimmt die für den Maschinen- und Anlagenbau wichtigen Teile des chinesischen Datensicherheitsgesetzes genauer unter die Lupe und gibt Empfehlungen für in China operierende Mitgliedsunternehmen.

https://www.vdma.org/viewer/-/v2article/render/17569547

19 Weiterbildungsangebote

Das Maschinenbau-Institut als Weiterbildungsakademie des VDMA bietet zum Thema Industrial Security ein breitgefächertes Weiterbildungsangebot, das nicht nur auf VDMA-Mitglieder beschränkt ist.

ISA-Qualifizierungsprogramm zum IEC 62443 Cybersecurity Expert

Die Quantität an Sicherheitsvorfällen nimmt auch im Maschinenbau stetig zu. Deshalb bietet das MBI in Kooperation mit der ISA Europe und in Zusammenarbeit mit dem Fraunhofer IOSB das offizielle Qualifizierungsprogramm zur Ausbildung von "Cybersecurity Experts" an.
In vier aufeinander aufbauenden Seminaren werden zudem die Schulungsinhalte der ISA ergänzt um spezifische Aspekte von vernetzten Maschinen und Anlagen. Für Fortgeschrittene gibt es den 5-tägigen Kompaktkurs direkt zum „Cybersecurity Expert“.

Security by Design für Maschinen und Anlagen

Cybersecurity bereits im Entwicklungsprozess mitdenken – das ist der Ansatzpunkt von Security by Design. Das Seminar wurde in Zusammenarbeit mit dem Fraunhofer IEM und Fraunhofer IOSB speziell für den Maschinenbau entwickelt und erläutert, wie die Prinzipien konkret angewendet werden müssen. Basis bilden die IEC 62443 und das VDMA Lastenheft zu Supply Chain Security.

Produktionsanlagen gegen Cyber-Bedrohungen schützen

In diesem Seminar werden Betreiber von industriellen Produktionssystemen in die Lage versetzt, diese vor Cyberangriffen und anderen Bedrohungen zu schützen. Es wird vermittelt, welche Maßnahmen gemäß der Normenreihe IEC 62443 ergriffen werden sollten.

Cyber-Krisenübung für den Maschinenbau

In diesem Seminar wird anhand eines Ransomware-Szenarios der Ernstfall bei einem Cyberangriff geübt und eine Blaupause für ein solides Krisenmanagement vermittelt.
Die rechtliche Vorgabe für ein adäquates Krisenmanagement erwartet Unternehmen mit der Umsetzung der NIS-2-Richtlinie. Unternehmen aus dem Maschinenbau und Anlagenbau, die zukünftig Cybersecurity-Vorgaben verpflichtend erfüllen müssen, können die Blaupause zur Umsetzung der Pflichten nutzen – ein wesentlicher Baustein für eine zukünftige NIS-2-Compliance.

Weitere Informationen unter:
https://www.maschinenbau-institut.de/themen/digitalisierung-innovation/

20 Impressum

VDMA
Lyoner Str. 18
60528 Frankfurt am Main
E-Mail: kommunikation@vdma.org
Internet: www.vdma.org

Erscheinungsjahr
2024

Bildnachweis
VDMA

Grafiken
VDMA

VDMA
Lyoner Str. 18
60528 Frankfurt am Main
Telefon +49 69 6603-0
E-Mail
kommunikation@vdma.org
Internet www.vdma.org

www.vdma.org