

WHITEPAPER

Erste Schritte zur Umsetzung der NIS-2 Richtlinie

Aufgrund der NIS-2 Richtlinie brauchen viele Unternehmen ein neues Cybersicherheitskonzept. Erfahren Sie in diesem Whitepaper, ob Ihre Organisation betroffen ist – und welche Maßnahmen Sie ergreifen können, um Ihre IT-Sicherheit den neuen gesetzlichen Anforderungen anzupassen.

Inhaltsverzeichnis

1	Einleitung	3
2	Basisinformationen zur NIS-2 Richtlinie	3
2.1	Welchem Zweck dient die NIS-2 Richtlinie?	4
2.2	Umsetzung auf nationaler Ebene	4
2.3	Fristen	4
3	Wer ist von der NIS-2 Richtlinie betroffen?	5
3.1	Kritische Infrastrukturen (KRITIS)	5
3.2	Besonders wichtige Einrichtungen	5
3.3	Wichtige Einrichtungen	5
	Infokasten: Betroffenheitsprüfung	6
3.4	Sanktionen bei Nichtbeachtung oder mangelhafter Umsetzung	6
	Infokasten: Auch Zulieferer betroffen	6
4	Maßnahmen zur Umsetzung der NIS-2 Richtlinie	7
	Infokasten: ISO-27001-zertifizierte Unternehmen im Vorteil	7
4.1	Überblick	8
4.2	Strategische Planung und Risikomanagement	8
4.3	Security Orchestration, Automation, and Response (SOAR)	8
	Praxisbeispiel: Automatisiertes Schwachstellenmanagement mit ACMP	9
4.4	Technische Sicherheitsmaßnahmen	9
4.5	Compliance und Reporting	9
	Praxisbeispiel: Dokumentation mit ACMP	10
4.6	Weitere Maßnahmen: Schulung, Vorfallmanagement und Kooperation	10
5	Die wichtigsten Maßnahmen auf einen Blick	11
6	Empfehlungen für Unternehmen	12
6.1	Sofortmaßnahmen: Schnell umsetzbare erste Schritte	12
6.2	Langfristige Strategie: Cybersicherheit nachhaltig verankern	12
6.3	Kooperation mit Experten: Externe Unterstützung einholen	12
7	Wie Aagon mit seinen Modulen die NIS-2 Umsetzung unterstützt	13
8	Anhang: Offizielle Quellen zur NIS-2 Richtlinie	14

1. Einleitung

Dieses Whitepaper richtet sich an Geschäftsführer und CTOs aus dem Mittelstand. Es enthält alle wichtigen Infos zur NIS-2 Richtlinie (Stand: Februar 2025), den erforderlichen Maßnahmen für betroffene Organisationen sowie praxisorientierte Empfehlungen zu deren Umsetzungen.



2. Basisinformationen zur NIS-2 Richtlinie

Die NIS-2 Richtlinie (Network and Information Security Directive) der Europäischen Union wurde am 05.12.2025 mit dem Bundesgesetzblatt Nr. 301 in deutsches Recht übernommen.

Sie zielt darauf ab, für EU-Länder ein hohes, gemeinsames Cybersicherheitsniveau zu gewährleisten.

Sie erweitert den Anwendungsbereich der ursprünglichen NIS-Richtlinie von 2016 und verpflichtet eine größere Anzahl von Unternehmen und Institutionen zur **Implementierung umfassender Sicherheitsmaßnahmen**.

In Deutschland betroffen sind insbesondere Betreiber sogenannter kritischer Infrastrukturen (KRITIS) sowie als „wichtig“ oder „besonders wichtig“ eingestufte Unternehmen (mehr dazu unter Punkt 3).

Die wichtigsten Neuerungen durch NIS-2:

- Erweiterter Geltungsbereich: Mehr Organisationen und Branchen sind von der Richtlinie betroffen
- Höhere Sicherheitsanforderungen: Unternehmen müssen umfassendere Cybersicherheitsmaßnahmen umsetzen
- Strengere Meldepflichten: Sicherheitsvorfälle müssen schneller und transparenter an Behörden gemeldet werden
- Schärfere Sanktionen: Unternehmen drohen hohe Geldstrafen, wenn sie die Vorgaben nicht erfüllen



2.1 Welchem Zweck dient die NIS-2 Richtlinie?

Die Hauptziele der Richtlinie sind:

- Stärkung der Widerstandsfähigkeit gegen Cyberangriffe in Europa
- Einführung einheitlicher Cybersicherheitsstandards in der EU
- Verbesserte Zusammenarbeit zwischen Mitgliedstaaten
- Striktere Sicherheits- und Meldepflichten, um effektiver auf Cyberbedrohungen reagieren zu können

Durch diese Maßnahmen soll das gesamte europäische Wirtschafts- und Verwaltungsumfeld besser vor Cyberbedrohungen geschützt werden.

2.2 Umsetzung auf nationaler Ebene

Die nationale Umsetzung der NIS-2 Richtlinie erfolgt in den EU-Mitgliedstaaten durch entsprechende Gesetze, die die erweiterten IT-Sicherheitsanforderungen in nationales Recht überführen. In Deutschland wird die Umsetzung der NIS-2 Richtlinie durch ein nationales Umsetzungsgesetz des Bundes geregelt, das bislang als NIS-2 Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) bekannt war.

2.3 Fristen

Der Gesetzesentwurf wurde am 22. Juli 2024 veröffentlicht und ist durch die Veröffentlichung im Bundesgesetz nun in Kraft getreten.

Betroffene Organisationen müssen sich jetzt mit NIS-2 beschäftigen und erforderliche Maßnahmen implementieren. Ein Sicherheitskonzept muss auf Anfrage von Behörden herausgegeben werden um empfindlichen Strafen zu entgehen.

3. Wer ist von der NIS-2 Richtlinie betroffen?

Durch die NIS-2 Richtlinie **erweitert sich der Kreis der Organisationen**, die die von der EU vorgegebenen Cybersicherheitsanforderungen erfüllen müssen.

Unterschieden wird dabei zwischen **kritischen Infrastrukturen (KRITIS)**, **wichtigen** Einrichtungen und **besonders wichtigen** Einrichtungen – die vom BSI neuerdings auch als „wesentliche“ und „wichtige“ Einrichtungen bezeichnet werden.

Ist Ihr Unternehmen betroffen? Die NIS-2 Betroffenheitsprüfung hilft Ihnen als Orientierungshilfe:

Betroffene Organisationen werden sich zudem proaktiv beim BSI registrieren müssen. Verbindliche Informationen zu diesem Prozess sind allerdings erst nach Abschluss des nationalen Gesetzgebungsverfahrens zu erwarten.

3.1 Kritische Infrastrukturen (KRITIS)

- Unternehmen mit essenzieller Bedeutung für Gesellschaft und Wirtschaft
- Branchen: Energie, Gesundheit, Transport, Wasser, Finanzwesen, Telekommunikation
- Bereits durch das IT-Sicherheitsgesetz reguliert
- Strenge Cybersicherheitsmaßnahmen und Meldepflichten vorgeschrieben

3.2 Besonders wichtige Einrichtungen

- Große Unternehmen mit hoher Relevanz für die öffentliche Sicherheit und Wirtschaft
- Branchen: Digitale Infrastruktur, [Bundesverwaltung](#), Lebensmittel, Chemie, Raumfahrt
- Verpflichtung zur Umsetzung umfassender Sicherheitsmaßnahmen
- Verpflichtung zur regelmäßigen Berichterstattung und Meldung von Sicherheitsvorfällen

3.3 Wichtige Einrichtungen

- Mitttelgroße Unternehmen
- Ähnliche Branchen wie „besonders wichtige“ Einrichtungen, aber mit geringerer Größe
- Weniger strenge, aber dennoch verpflichtende Sicherheitsmaßnahmen
- Verpflichtung zur Einführung eines Risikomanagements für Cybersicherheit



Betroffenheitsprüfung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet eine **Betroffenheitsprüfung** an. Organisationen können damit schnell und unkompliziert prüfen, ob und in welchem Ausmaß sie von den neuen NIS-2 Cybersicherheitsanforderungen betroffen sind.

3.4 Sanktionen bei Nichtbeachtung oder mangelhafter Umsetzung

Organisationen, die die Anforderungen der NIS-2 Richtlinie bis zum Inkrafttreten des neuen Umsetzungsgesetzes nicht erfüllen, müssen mit **empfindlichen Strafen** rechnen:

- **Bußgelder:** Bis zu 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist)
- **Haftung der Geschäftsführung:** Unter Umständen persönliche Verantwortung für die Einhaltung der NIS-2 Cybersicherheitsanforderungen
- **Eingriffsmaßnahmen der Behörden:** Anordnungen zur Nachbesserung oder im Extremfall Betriebsuntersagung

Betroffene Organisationen **müssen bereits jetzt die nötigen Maßnahmen ergreifen**, um die neuen Anforderungen rechtzeitig zu erfüllen und auf mögliche behördliche Kontrollen vorzubereitet zu sein.



Auch Zulieferer betroffen

Nicht nur direkt regulierte Unternehmen müssen sich mit den Anforderungen der NIS-2 Richtlinie befassen. Auch **Zulieferer oder Dienstleister für kritische Einrichtungen können indirekt betroffen sein**, da Unternehmen nachweisen müssen, dass ihre Partner in der Lieferkette ausreichende Cybersicherheitsmaßnahmen ergriffen haben.

4. Maßnahmen zur Umsetzung der NIS-2 Richtlinie

Disclaimer

Aufgrund der Komplexität des Themas und derzeit noch vorhandener Unklarheiten hinsichtlich der konkreten Gesetzgebung in Deutschland erhebt Aagon keinen Anspruch auf eine vollständige Darstellung aller nötigen Maßnahmen für alle betroffenen Organisationen. Die nachfolgenden Informationen sind als allgemeiner Einstieg in das Thema NIS-2 Umsetzung zu verstehen.

Für viele Unternehmen ist die Umsetzung der NIS-2 Anforderungen eine Herausforderung – ob in organisatorischer, personeller und finanzieller Hinsicht.

Zwar zeigt eine Studie von Juni 2024, dass 80% der befragten europäischen IT-Führungskräfte zuversichtlich sind, die NIS-2 Anforderungen fristgerecht umsetzen zu können. Jedoch glauben nur 53%, dass ihre Teams diese vollständig verstehen. 56% geben zudem an, dass die IT-Teams von der Führungsebene nicht die notwendige Unterstützung für die fristgerechte Umsetzung erhalten.

Entsprechend wichtig ist eine sorgfältige Planung und Ressourcenzuweisung für die erfolgreiche und rechtzeitige Umsetzung der erforderlichen Maßnahmen. Der Aufwand kann je nach Einstufung (KRITIS, „wesentlich“ oder „wichtig“), Unternehmensgröße, Branche und bereits vorhandenen Sicherheitskonzepten erheblich variieren.

ISO-27001-zertifizierte Unternehmen im Vorteil



ISO 27001-zertifizierte Unternehmen sind bei der Umsetzung von NIS-2 klar im Vorteil, da sie bereits ein strukturiertes ISMS (Informationssicherheits-Managementsystem), Risikomanagement und Dokumentationsprozesse etabliert haben. Viele der durch NIS-2 geforderten technischen und organisatorischen Maßnahmen, wie Zugangskontrollen und Incident Management, sind bereits vorhanden. Zudem sind sie durch regelmäßige Audits bestens auf die strenger behördlichen Prüfungen und Meldepflichten vorbereitet. Der Anpassungsaufwand ist dadurch deutlich reduziert.

4.1 Überblick

Betroffene Organisationen müssen sich sowohl auf der strategischen als auch auf der technischen und organisatorischen Ebene mit der Umsetzung der NIS-2 Richtlinie auseinandersetzen. Während strategische Maßnahmen auf eine ganzheitliche Sicherheitsplanung und Risikobewertung abzielen, umfassen technische Maßnahmen konkrete Schutzmaßnahmen für IT-Systeme und Netzwerke. Ergänzend sind organisatorische Maßnahmen erforderlich, um Meldepflichten einzuhalten, Mitarbeiter für das Thema Cybersicherheit zu sensibilisieren und eine effektive Reaktion auf Sicherheitsvorfälle zu ermöglichen.

Die nachfolgenden Abschnitte geben eine strukturierte Übersicht über diese drei zentralen Aspekte.

4.2 Strategische Planung und Risikomanagement

Die erfolgreiche Umsetzung der NIS-2 Richtlinie beginnt mit einer strukturierten Sicherheitsstrategie. Unternehmen müssen ein umfassendes Risikomanagement etablieren, um Schwachstellen zu identifizieren und gezielte Sicherheitsmaßnahmen abzuleiten. Eine fundierte Sicherheitsstrategie sorgt dafür, dass Cybersicherheit nicht isoliert betrachtet wird, sondern integraler Bestandteil der Unternehmensstrategie ist.

Wichtige Schritte im Risikomanagement:

- **Identifikation kritischer Geschäftsprozesse:** Welche IT-Systeme und Prozesse sind unverzichtbar?
- **Analyse der Bedrohungslage:** Welche internen und externen Risiken bestehen?
- **Bewertung von Schwachstellen:** Wo gibt es potenzielle Sicherheitslücken?
- **Entwicklung einer Sicherheitsstrategie:** Definition von Schutzziele und Priorisierung von Maßnahmen

4.3 Security Orchestration, Automation, and Response (SOAR)

Das **SOAR-Konzept** (Security Orchestration, Automation, and Response) hilft Unternehmen, Sicherheitsvorfälle schneller zu erkennen, automatisiert darauf zu reagieren und administrative Prozesse zu entlasten.

Warum SOAR?

- Automatisierte Schwachstellenerkennung und -behebung
- Orchestrierte Reaktion auf Bedrohungen, z. B. durch automatische Quarantäne infizierter Systeme
- Filterbasierte Automatisierung zur kontinuierlichen Absicherung gegen wiederkehrende Bedrohungen



Praxisbeispiel:

Automatisiertes Schwachstellenmanagement mit ACMP

Ein Unternehmen mit 500 verteilten Clients stellt eine kritische Sicherheitslücke in der Open-Source-Software 7-Zip fest. Mit **ACMP Schwachstellenmanagement** kann der Administrator alle betroffenen Systeme identifizieren und die Sicherheitslücke automatisiert schließen:

1. Die betroffene Version wird über die Schwachstellendatenbank erkannt
2. Ein Filter erstellt automatisch eine Gruppe aller betroffenen Clients
3. Ein verknüpftes **Managed Software**-Paket aktualisiert 7-Zip auf allen relevanten Systemen
4. Die Automatisierung stellt sicher, dass auch später eingeschaltete Geräte das Update erhalten

Der Prozess reduziert manuellen Aufwand und ermöglicht eine **effiziente und automatisierte Standardreaktion** auf Cyberbedrohungen.

4.4 Technische Sicherheitsmaßnahmen

Neben der strategischen Planung sind gezielte technische Maßnahmen erforderlich, um die Anforderungen der NIS-2 Richtlinie zu erfüllen.

Wichtige Maßnahmen:

- **Netzwerksicherheit:** Firewalls, Intrusion-Detection-Systeme, Zero-Trust-Prinzip
- **Zugriffsmanagement:** Multi-Faktor-Authentifizierung, Least Privilege-Prinzip
- **Patch-Management:** Automatisierte Updates, regelmäßige Schwachstellenscans
- **Datenverschlüsselung:** Schutz sensibler Informationen mit BitLocker-Management

4.5 Compliance und Reporting

Die NIS-2 Richtlinie erfordert eine umfassende Dokumentation aller Sicherheitsmaßnahmen. Unternehmen müssen jederzeit nachweisen können, dass ihr Sicherheitskonzept den gesetzlichen Anforderungen entspricht.



Praxisbeispiel:

Automatisiertes Lizenzmanagement mit ACMP

Softwarelizenzierung ist ein essenzieller Bestandteil der IT-Sicherheitsstrategie eines Unternehmens. Ungültige oder fehlende Lizenzen können nicht nur hohe Kosten durch Nachlizenzierungen verursachen, sondern auch Sicherheitsrisiken darstellen, da nicht lizenzierte Software oft keine Updates erhält. Gerade in Unternehmen mit vielen Arbeitsplätzen ist eine manuelle Verwaltung kaum praktikabel. Ein automatisiertes System wie **ACMP Lizenzmanagement** schafft hier Transparenz und minimiert Risiken.

1. ACMP erfasst installierte Software und gleicht sie mit vorhandenen Lizenzen ab.
2. Automatische Reports zeigen Unterlizenzierungen oder auslaufende Lizenzen auf.
3. Administratoren erhalten Warnmeldungen bei nicht lizenzierter Software oder auslaufenden Lizenzen.
4. Lückenlose Dokumentation unterstützt die Einhaltung der NIS-2-Anforderungen.

ACMP reduziert durch Automatisierung den manuellen Aufwand, erhöht die IT-Sicherheit und sorgt für eine rechtskonforme Lizenzverwaltung.

4.6 Weitere Maßnahmen: Schulung, Vorfallmanagement und Kooperation

Ergänzend zur technischen Absicherung sind organisatorische Maßnahmen erforderlich, um Sicherheitsstrategien konsequent umzusetzen:

- **Mitarbeiterschulungen:** Sensibilisierung für Cybersicherheitsrisiken und regelmäßige Phishing-Simulationen
- **Vorfallmanagement:** Definition klarer Prozesse für die Reaktion auf Cyberangriffe
- **Kooperation mit dem BSI:** Nutzung von Sicherheitswarnungen und Informationsaustausch zur Bedrohungslage



5. Die wichtigsten Maßnahmen auf einen Blick

- 1 Betroffenheitsprüfung durchführen**
 - Mithilfe der BSI-Betroffenheitsprüfung können Organisationen feststellen, ob und in welchem Ausmaß sie von den NIS-2 Regelungen betroffen sind
- 2 Risikomanagement etablieren**
 - Schwachstellen bewerten und eine umfassende Cybersicherheitsstrategie auf Basis von Bedrohungsszenarien entwickeln
- 3 Technische Maßnahmen umsetzen**
 - Netzwerksicherheit, Verschlüsselung und Zugriffsmanagement als essenzielle Bausteine implementieren
 - Patch-Management und Datensicherungen in den Sicherheitsprozess integrieren
- 4 Meldepflichten beachten**
 - Sicherheitsvorfälle müssen innerhalb von 24 bis 72 Stunden an die zuständigen Behörden gemeldet werden
 - Ein strukturiertes Incident-Response-Management hilft, die Meldepflicht effizient zu erfüllen
- 5 Mitarbeiterschulungen & Sensibilisierung sicherstellen**
 - Regelmäßige Awareness-Trainings und Phishing-Simulationen reduzieren Sicherheitsrisiken durch menschliche Fehler
 - Cybersicherheit muss fester Bestandteil der Unternehmenskultur werden
- 6 Regelmäßige Audits & Compliance-Berichte führen**
 - Dokumentation und Berichterstattung sind essenziell für die Nachweispflicht gegenüber Aufsichtsbehörden
 - Unternehmen sollten regelmäßig interne Audits und externe Prüfungen durchführen

6. Empfehlungen für Unternehmen

Die Umsetzung der NIS-2 Richtlinie ist keine einmalige Aufgabe, sondern ein kontinuierlicher Prozess. Betroffene Organisationen sollten im eigenen Interesse frühzeitig mit der Planung und Implementierung der erforderlichen Maßnahmen beginnen, um Fristen einzuhalten und Sicherheitsrisiken zu minimieren.

Sie sollten die strategische Integration von Cybersicherheit dabei nicht in erster Linie als gesetzliche Anforderung sehen, sondern als Investition in die eigene IT-Resilienz – und in das langfristige Vertrauen von Kunden und Partnern.

6.1 Sofortmaßnahmen: Schnell umsetzbare erste Schritte

- Verantwortlichkeiten klären: Wer ist für die NIS-2 Umsetzung im Unternehmen zuständig?
- Risikobewertung durchführen: Wo gibt es potenzielle Sicherheitslücken?
- Technische Mindestanforderungen umsetzen: Firewall, Zugriffskontrollen, Backups
- Meldeprozesse definieren: Wer meldet Vorfälle und wie erfolgt die Kommunikation mit Behörden?

6.2 Langfristige Strategie: Cybersicherheit nachhaltig verankern

- Sicherheitsstrategie in Unternehmensprozesse integrieren: IT-Sicherheit als Teil der Geschäftsstrategie
- Automatisierung nutzen: SOAR-Tools implementieren, um Sicherheitsprozesse effizient zu gestalten
- Lieferketten-Compliance sicherstellen: Verträge mit Dienstleistern auf NIS-2 Konformität überprüfen
- Cyber-Resilienz aufbauen: Notfallpläne regelmäßig testen und optimieren

6.3 Kooperation mit Experten: Externe Unterstützung einholen

- Zusammenarbeit mit IT-Sicherheitsfirmen: Externe Experten helfen, Compliance effizient umzusetzen
- Nutzung von Managed Security Services (MSS): Sicherheitsmaßnahmen auslagern, wenn interne Ressourcen fehlen
- Austausch mit Behörden und Branchenpartnern: Frühzeitige Informationen über Bedrohungen erhalten

7. Wie Aagon mit seinen Modulen die NIS-2 Umsetzung unterstützt

Die Einhaltung der NIS-2 Richtlinie erfordert sowohl strategische als auch technische und organisatorische Maßnahmen, um IT-Sicherheitsrisiken zu minimieren und Compliance sicherzustellen. Aagon bietet durch die individuelle Kombination von ACMP-Modulen eine für unzählige Anwendungsfälle konfigurierbare Lösung, die Unternehmen bei der Umsetzung der NIS-2 Anforderungen in mehreren Schlüsselaspekten unterstützt:

Module, die bei der Umsetzung unterstützen:



ACMP Defender Management

Zentralisierte Verwaltung von Windows Defender sorgt für mehr Cybersicherheit.



ACMP Core

Unser Basis-Modul, Grundlage für ein umfassendes Konzept.



ACMP Lizenzmanagement

Bringt Transparenz in Ihre Softwarelizenzen und minimiert Risiken durch unlizenzierte Software.



ACMP Desktop Automation

Einheitliche Standards durch automatisierte Softwareverteilung und Task-Management.



ACMP Complete Aagon Windows Update Management

Effektive Verwaltung von Windows-Updates sichert Ihre IT kontinuierlich gegen Schwachstellen ab.



ACMP Managed Software

Automatisiertes Patch-Management schließt Sicherheitslücken in Drittanbieter-Software schnell und zuverlässig.



ACMP BitLocker Management

Zentralisierte Verwaltung der BitLocker-Verschlüsselung schützt vor unberechtigtem Zugriff auf Daten.



ACMP Schwachstellenmanagement

Identifiziert Sicherheitslücken zur Absicherung Ihrer IT-Systeme.

Jetzt Kontakt aufnehmen

Wenn Sie von NIS-2 betroffen sind und die Anforderungen noch nicht umgesetzt haben, sollten Sie keine weitere Zeit verlieren. Beginnen Sie jetzt damit, Ihre IT-Sicherheitsinfrastruktur effizient und automatisiert zu verwalten und ihre IT-Sicherheitsprozesse im eigenen Interesse nachhaltig zu optimieren.

Für Fragen aller Art stehen Ihnen unsere IT-Security-Experten jederzeit zur Verfügung!

8. Anhang: Offizielle Quellen zur NIS-2 Richtlinie

Hier ist eine Liste aller verwendeten Links und Quellen für das Whitepaper:

-  [Offizielle EU-Website zur NIS-2 Richtlinie](#)
-  [Bundesamt für Sicherheit in der Informationstechnik \(BSI\) – Informationen zur NIS-2 Richtlinie](#)
-  [NIS-2 Betroffenheitsprüfung des BSI](#)
-  [Bundesgesetz zur Umsetzung der NIS-2 Richtlinie \(NIS2UmsuCG\)](#)
-  [Studie zur Umsetzung der NIS-2 Richtlinie in europäischen Unternehmen \(Zscaler, Juni 2024\)](#)
-  [Aagon NIS-2 Lösungsseite für Unternehmen](#)



ÜBER AAGON

„Manage any device in a connected world!“ – Aagon entwickelt seit 30 Jahren Client-Management- und -Automation-Lösungen und ist der Spezialist für die Verwaltung von Endgeräten und die Automatisierung von Standardaufgaben. Durch sorgfältige Entwicklungen, mehr als 20 Jahre Marktreife und die enge Zusammenarbeit mit unseren Kunden und Partnern sind unsere Produkte perfekt auf Ihre Anforderungen und Bedürfnisse zugeschnitten.

Individuelle Beratung und die beste Unterstützung von Kunden und Partnern bei der Installation und ersten Einrichtung gehören deshalb zum Standard von Aagon. Ein umfassendes Verständnis von Kundenbedürfnissen und der ständige Kontakt zu unseren Kunden und Partnern ermöglichen Softwareentwicklung auf Augenhöhe.

Webinare-on-Demand, zahlreiche Whitepaper und die beliebten Treffen zum Anwendertreffen an Standorten in ganz Deutschland sind nur drei Beispiele, wie nahe am Kunden ACMP wirklich entwickelt wird.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.



GOLD
UNIFIED ENDPOINT MANAGEMENT
IP
INSIDER
AWARD
2025

techconsult | TECHNOLOGY MARKET ANALYSTS | heise group
 **PUR 2025**
Professional User Rating
★ **5-FACH** ★
★ **CHAMPION** ★

EIN PRODUKT DER

Aagon GmbH

Lange Wende 33

D-59494 Soest

Fon: +49 (0)2921 - 789200

Fax: +49 (0)2921 - 789244

sales@aagon.com

www.aagon.com