Bild: 1903750670 ©Rayn, generiert mit KI, www.stock.adobe.com

Cybersicherheit in der Massivumformung ist jetzt Chefsache – Warum eine Firewall allein nicht mehr reicht

Die Schonfrist ist endgültig abgelaufen: Mit der neuen EU-Richtlinie NIS2 (Network and Information Security Directive 2) und dem entsprechenden nationalen Gesetz gelten deutlich strengere Regeln für die IT-Sicherheit in vielen Betrieben des verarbeitenden Gewerbes. Wer die neuen Vorgaben ignoriert, riskiert nicht nur verheerende Cyberangriffe und Lieferkettenausfälle, sondern auch persönliche Haftung der Geschäftsführung und hohe Strafen. Für wen die neuen Registrierungs- und Meldepflichten im Detail gelten, wie der Aufbau eines Managementsystems funktioniert und warum die Geschäftsleitung das Thema ab sofort nicht mehr an die IT-Abteilung abschieben darf, erklären wir im ausführlichen Interview.

INTERVIEWPARTNER

Dipl.-Ing.
Karsten Kunde

ist Geschäftsführer
der 1or2 Business-Development-Beratung
in Wipperfürth

Das Jahr 2026 bringt für viele Betriebe der Zulieferindustrie eine regulatorische Umstellung: Das Gesetz NIS2 verpflichtet rund 30.000 Unternehmen, umfangreiche Risikomanagement-, Registrierungs- und Meldeprozesse zu installieren beziehungsweise ihre Strukturen auf den Stand der Technik zu bringen. Die Registrierungsfrist für betroffene Unternehmen in Deutschland ist am 6. März 2026 abgelaufen. Registriert haben sich aber erst rund 11.500 Behörden, Unternehmen und andere kritische Einrichtungen, meldet der Branchendienst „Heise". Wahrscheinlich, weil sie nicht mal wüssten, dass ihre Company unter das neue Gesetz fällt.

Wir befragten Karsten Kunde, Experte für Informationssicherheit und Geschäftsführer des Beratungsunternehmens 1or2, warum die Zeit für die Unternehmen extrem drängt und welche Schritte metallverarbeitende Betriebe jetzt bis ins kleinste Detail umsetzen müssen.

? Das Thema Cybersicherheit begleitet die Wirtschaft schon lange, und Hackerangriffe sind fast an der Tagesordnung. Warum sorgen die NIS2-Richtlinie und ihre Überführung in das deutsche BSI-Gesetz (BSIG) gerade jetzt, Anfang 2026, für derart viel Aufsehen und Nervosität in den Chefetagen?

! Das liegt daran, dass es jetzt rechtlich absolut ernst wird und extrem harte, kurzfristige Deadlines gelten. Die EU-Richtlinie NIS2 wurde auf europäischer Ebene verabschiedet, um die Sektoren, die kritische Infrastrukturen und essenzielle Dienste bereitstellen, massiv auszuweiten und die Lieferkettenresilienz in ganz Europa zu erhöhen. Weitere Ziele sind: die Zusammenarbeit innerhalb der EU vereinfachen und empfindliche Strafen einführen.

Der deutsche Gesetzgeber hat dies im NIS2-Umsetzungsgesetz (NIS2UmsuCG) in das BSI-Gesetz überführt. Das Gesetz trat am 6. Dezember 2025 in Kraft. Exakt einen Monat später, am 6. Januar 2026, wurde das Meldeportal des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für die Registrierung live geschaltet. Und hier tickt die Uhr extrem schnell: Betroffene Unternehmen müssen sich innerhalb von drei Monaten nach Inkrafttreten des Gesetzes registrieren. Das bedeutet: Das Ende der Frist für die Registrierung fällt auf den 6. März 2026. Wer sich bisher nicht gekümmert hat, ist im Verzug. Ein Verstoß gegen diese gesetzliche Registrierungspflicht nach § 33 wird bereits als Ordnungswidrigkeit gewertet.

? Betrifft das denn überhaupt klassische Betriebe der Massivumformung? In der Branche hört man oft den Satz: „Wir schmieden Stahl und bauen keine Kraftwerke – wir sind doch gar keine kritische Infrastruktur (KRITIS)"?

! Die ist ein sehr gefährlicher Trugschluss. Es stimmt: Automatisch klassische KRITIS-Unternehmen nach dem BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) sind metallverarbeitende Unternehmen erst einmal nicht. Es wäre aber völlig falsch, sich pauschal in Sicherheit zu wiegen, denn die Richtlinie hat den Geltungsbereich extrem ausgeweitet. Neben den bekannten KRITIS-Sektoren gibt es nun die verbindlichen Einstufungen „Besonders wichtige Einrichtungen" nach Anlage 1 und „Wichtige Einrichtungen" nach Anlage 2. Man muss im Einzelfall zwingend prüfen, ob man betroffen ist.

Und hier kommt für viele das böse Erwachen: Unter die Anlage 2 fällt unter Punkt 5 explizit das „Verarbeitende Gewerbe/Her-

KI-generiert

stellung von Waren". Ein Massivumformer kann somit als „wichtige Einrichtung" eingestuft werden, wenn das Unternehmen mindestens 50 Mitarbeiter beschäftigt oder beim Umsatz eine bestimmte Schwelle überschreitet: entweder einen Umsatz von nnnnn Euro (klären) oder eine Bilanzsumme von mindestens 10 Millionen Euro erreicht.

Können Sie das an konkreten Produkten der Massivumformung festmachen?

Ja, Anlage 2 führt das Verarbeitende Gewerbe beziehungsweise die Herstellung von Waren sehr genau aus und nennt auch eindeutige NACE-Codes zur Einordnung der betroffenen Unternehmen.

1. Herstellung von Medizinprodukten und Invitro-Diagnostika
2. Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen NACE 26
3. Von elektrischen Ausrüstungen NACE 27
4. Maschinenbau NACE 28
5. Kraftwagen und Kraftwagenteilen NACE 29
6. Sonstiger Fahrzeugbau NACE 30

Wenn sich ein Massivumformer also als Automobilzulieferer einstuft, fällt er in die NACE 29 und damit automatisch unter die NIS2-Richtlinie. Genau diese Einstufung, also ob ein Unternehmen tatsächlich unter NACE 29 fällt oder nicht und somit als „wichtiges Unternehmen" gemäß NIS2 gilt, ist häufig Gegenstand langwieriger Diskussionen. Allerdings lässt sich die Frage auch pragmatischer betrachten: Wo liegt das größere Risiko – in der Registrierung oder darin, sich nicht zu registrieren? Diese Abwägung sollten wir am besten ganz am Ende treffen, wenn wir alle Anforderungen aus der NIS2-Richtlinie vollständig durchgegangen sind.

Oftmals sind solche sperrigen und komplexen IT-Themen im Management unbeliebt und werden gerne mit einem knappen Budget an den IT-Leiter delegiert. Geht das bei NIS2 noch?

Das ist genau das typische Problem, das wir in der Praxis tagtäglich beobachten. Das Management hat selbstverständlich ein großes Interesse daran, den laufenden Geschäftsbetrieb ohne Störungen sicherzustellen. Gleichzeitig sehen wir jedoch nur wenig Bereitschaft, zusätzliche Ressourcen – insbesondere die eigene Zeit der Geschäftsführung – in das Thema Informationssicherheit zu investieren. Die Tendenz, dieses Thema vollständig an die IT-Abteilung zu delegieren, ist enorm hoch. Paradoxerweise müsste gerade das Management ein besonderes Interesse daran haben, das Unternehmen durch geeignete Maßnahmen bestmöglich abzusichern.

Und genau hier zieht NIS2 eine dicke rote Linie: Das Wegdelegieren funktioniert rechtlich nicht mehr. § 38 des Gesetzes nimmt die Geschäftsführung explizit und persönlich in die Verantwortung. Die Geschäftsleitungen wichtiger und besonders wichtiger Einrichtungen sind gesetzlich verpflichtet, die notwendigen Risikomanagementmaßnahmen nach § 30 nicht nur umzusetzen, sondern deren Umsetzung auch persönlich zu überwachen. Mehr noch: Absatz 3 verpflichtet die Chefetage dazu, regelmäßig an speziellen Schulungen teilzunehmen. Die Geschäftsführung muss ausreichende Kenntnisse und Fähigkeiten erlangen, um Risiken in der Informationstechnik zu erkennen und deren Auswirkungen auf die vom Unternehmen erbrachten Dienste fundiert beurteilen zu können. Cybersecurity ist jetzt unweigerlich Chefsache.

Was droht, falls ein Geschäftsführer das ignoriert, das Budget für IT-Sicherheit streicht oder Fristen verstreichen lässt?

In diesem Fall können empfindliche Strafen drohen. Bei Verstößen gegen die Risikomanagementmaßnahmen nach § 30 oder gegen die Meldepflichten nach § 31 greift § 60, und der regelt die Strafen. Für „wichtige Einrichtungen" drohen Strafen von bis zu 7 Millionen Euro oder 1,4 Prozent des weltweiten Umsatzes.

Lassen Sie uns über die Registrierung sprechen. Wie genau läuft diese ab? Ist das ein simples Online-Formular?

Grundsätzlich ja – mit der richtigen Vorbereitung ist die Registrierung schnell und unkompliziert erledigt. Sie erfolgt über das BSI-Meldeportal (portal.bsi.bund.de). Das Wichtigste vorweg: Für die Authentifizierung ist zwingend ein ELSTER-Login erforderlich, also eine gültige Zertifikatsdatei samt Passwort. Im Portal müssen Sie dann umfassende Angaben zum Unternehmen machen: Name, Rechtsform, das Register (inklusive Art, Nummer und Registergericht) sowie Unternehmenswebseite. Besonders relevant

KI-generiert

sind die Einstufungskriterien. Hier müssen Sie die Mitarbeiterzahl (unter 50 oder unter 250) sowie den Jahresumsatz (unter 10 Mio. oder unter 50 Mio. Euro) angeben. Außerdem wählen Sie den passenden Sektor und die Branche aus vorgegebenen Auswahlfeldern aus.

Zusätzlich verlangt das BSI die Angabe aller öffentlichen IP-Adressen des Unternehmens Und ganz wichtig: Es muss eine Kontaktstelle benannt werden, die immer erreichbar ist, beispielsweise über eine Funktions-E-Mail. Auch die zuständigen Aufsichtsbehörden des Bundes müssen angegeben werden.

Angenommen, ein betroffener Betrieb der Massivumformung hat sich registriert und will jetzt inhaltlich alles richtig machen. Kann man nicht einfach eine gute Sicherheitssoftware oder Hardware kaufen und das Thema abhaken?

Eindeutig nein! Es gibt schlichtweg kein Produkt, das ich einfach kaufe und dann automatisch die NIS2-Anforderungen erfüllt. Was Unternehmen nach § 30 aufbauen müssen, ist ein Informationssicherheits-Managementsystem.

Dabei fordert das Gesetz geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der IT-Systeme zu vermeiden. Zu berücksichtigen sind bei der Verhältnismäßigkeit das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen.

Welche Maßnahmen fordert § 30 des Gesetzes denn konkret von den Betrieben?

Der Maßnahmenkatalog ist sehr umfangreich, muss den Stand der Technik einhalten und auf einem gefahrenübergreifenden Ansatz beruhen. Er umfasst mindestens Konzepte in Bezug auf die Risikoanalyse und Sicherheit in der Informationstechnik, die Bewältigung von Sicherheitsvorfällen und ganz wichtig: die Sicherheit der Lieferkette. Letzteres schließt sicherheitsbezogene Aspekte der Beziehungen zu unmittelbaren Anbietern ein.

Zudem müssen sie sich um die Aufrechterhaltung des Betriebs kümmern, also ein Backup-Management und Konzepte für die Wiederherstellung nach einem Notfall – ein sogenanntes Krisenmanagement – etablieren. Das Gesetz fordert darüber hinaus Konzepte für den Einsatz von Kryptografie und Verschlüsselung, grundlegende Verfahren zur Cyberhygiene und Schulungen, Sicherheit des Personals durch Zugriffskontrollen und den verpflichtenden Einsatz von Multi-Faktor-Authentifizierung (MFA) sowie gesicherter Sprach-, Video- und Textkommunikation innerhalb der Einrichtung. Auch das Schwachstellenmanagement bei der Wartung von IT-Systemen gehört zwingend dazu. All das muss dokumentiert werden.

Das ist ein enormer Berg an Anforderungen. Wie verhält sich NIS2 zu bestehenden Standards wie ISO 27001 oder TISAX, die in der Automobilindustrie ja stark verbreitet sind?

NIS2 orientiert sich an diesen internationalen Standards, verweist aber bei uns in der Ausgestaltung immer wieder auf das BSI. Ein Zertifikat schützt Sie rechtlich nicht vor NIS2, aber die Forderungen an das Managementsystem sind sehr ähnlich. Wer bereits ISO 27001 oder TISAX im Unternehmen etabliert hat, hat eine hervorragende Basis, um die NIS2-Compliance zu erreichen.

Stichwort Ernstfall: Was fordert NIS2, wenn ein Unternehmen der Massivumformung tatsächlich gehackt wird, beispielsweise durch Ransomware?

§ 32 BSIG regelt die Meldepflichten sehr strikt, und hier müssen Sie extrem schnell reagieren. Es gilt eine strenge, mehrstufige Meldepflicht beim BSI:

1. Frühe Erstmeldung: Diese muss bereits innerhalb der ersten 24 Stunden nach Kenntniserlangung eines Sicherheitsvorfalls erfolgen.
2. Bestätigung und Aktualisierung: Unverzüglich, spätestens aber innerhalb der ersten 72 Stunden, muss eine Bestätigung und Aktualisierung der Erstmeldung erfolgen. Das Bundesamt kann zudem jederzeit Zwischenmeldungen anfragen.
3. Abschlussbericht: Spätestens nach einem Monat muss ein detaillierter Bericht eingereicht werden (oder ein Bericht des fortlaufenden Zustands).

	Betreiber kritischer Anlagen	Besonders wichtige Einrichtung	Wichtige Einrichtung
Zusätzliche Anforderungen für KRITIS	✓		
§ 33 Registrierung	✓	✓	✓
§ 30 Risikomanagementmaßnahmen Aufbau eines ISMS	✓	✓	✓
§ 61 § 62 Nachweise	✓	▪ Einzelfall Anordnung ▪ Grundsätzliche Pflicht kann noch kommen ohne Gesetzesänderung	▪ Verdacht aufgrund von Tatsachen
§ 32 Meldepflichten	✓	✓	✓
§ 35 Unterrichtungspflichten (Kunden)	✓	✓	✓
§38 Verantwortung Geschäftsführung	✓	✓	✓
$65 Strafen	✓	✓	✓

Anforderungen je Einordnung aus Gesetz, Bild: 1or2

	ISO 27001	TISAX	BSI IT-Grundschutz	NIS2
Verbreitung	International	International	Deutschland	Europa
Detaillierung	hoher Freiheitsgrad (ws)	hoher Freiheitsgrad (was)	sehr detailliert (was und wie)	hoher Freiheitsgrad (Aber Aussicht ist das BSI)
Branche	branchenunabhängig (Verbreitet im IT-Bereich)	Automobilbranche	branchenunabhängig (für Bundesbehörden verpflichtend)	branchenunabhängig
Zertifizierung	verschiedene akkreditierte Stellen	verschiedene akkreditierte Stellen	ausschließlich über BSI	Abhängig von der Einstufung Aber wahrscheinlicher bei einem IT-Sicherheitsvorfall
Überwachung	jährlich	Follow-Up Termine	jährlich	
Re-Zertifizierung	alle 3 Jahre	alle 3 Jahre	alle 3 Jahre	
Bewertung	Mit High-Level-Structure wie alle ISO X001 Managementsystemnormen zur leichteren Integration in ein IMS	Basiert auf der Abarbeitung des VDA ISA 6 Fragebogens. Der ist eine Weiterentwicklung des Anhangs der DIN ISO 27001.	Es ist möglich ISO 27001 nach den Vorgaben der BSI-Standards 200-1 bis 200-4 zu erfüllen. Sehr viel konkreter als 27001.	Orientierung an internationale Standards aber immer wieder Verweis auf BSI

Überblick der ISMS-Standards gegenüber NIS2, Bild: 1or2

Dieser Abschlussbericht erfordert eine ausführliche Beschreibung des Sicherheitsvorfalls, die Angabe der Art der Bedrohung beziehungsweise der zugrundeliegenden Ursache, die Dokumentation der getroffenen und laufenden Maßnahmen sowie die Bewertung von eventuellen grenzüberschreitenden Auswirkungen. Das schaffen Sie in der Kürze der Zeit nur, wenn Sie vorher saubere Meldeprozesse etabliert haben.

? Wie wird das Einhalten der NIS2 Richtlinie überwacht?

! Bei wichtigen Einrichtungen erfolgt die Überwachung nach dem Kernprinzip der Reaktiven Überwachung, also die sogenannte Expost-Aufsicht (anlassbezogene Aufsicht). Das bedeutet: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) überwacht die Unternehmen nicht proaktiv. Es gibt keine anlasslosen Vor-Ort-Kontrollen.

Sie müssen keine regelmäßigen Nachweise (wie zum Beispiel alle drei Jahre ein Audit-Zertifikat) unaufgefordert beim BSI einreichen. Das BSI wird bei wichtigen Einrichtungen in der Regel erst dann aktiv, wenn ein konkreter Anlass vorliegt. Ein solcher Anlass ist meist:

- Ein meldepflichtiger Sicherheitsvorfall (beispielsweise ein erfolgreicher Ransomware-Angriff), den Sie dem BSI gemeldet haben.
- Konkrete Hinweise oder Beschwerden, dass Ihr Unternehmen die gesetzlichen Vorgaben (beispielsweise zum Risikomanagement) nicht einhält.

Sobald das BSI aufgrund eines Vorfalls oder Hinweises aktiv wird, gibt es sehr weitreichende Befugnisse, um die Einhaltung der Gesetze nachträglich zu überprüfen.

? Haben Sie einen abschließenden Rat an die Unternehmen der Branche, die jetzt vielleicht überfordert sind?

! Sehen Sie es nicht nur als lästige Pflicht, sondern sehen Sie NIS2 als Chance, das Thema Informationssicherheit richtig anzugehen.

Wenn man sich vor Augen führt, dass NIS2 im Kern nur das verlangt, was ohnehin auf der Todo-Liste vieler Unternehmen steht – oder idealerweise bereits umgesetzt ist –, verliert auch die Frage, ob man sich registrieren sollte oder nicht, an Bedeutung. Einen schwerwiegenden Sicherheitsvorfall, etwa einen Hackerangriff, vor dem BSI zu verbergen, wird in der Praxis kaum möglich sein. In einem solchen Fall hätte man neben dem eigentlichen Angriff zusätzlich einen Verstoß gegen die NIS2-Richtlinie zu verantworten.

Die eigene Position wäre dann deutlich geschwächt, insbesondere wenn die geforderten Risikomanagementmaßnahmen nicht vollständig oder nicht korrekt umgesetzt wurden. Denn wäre das Risikomanagement ordnungsgemäß etabliert gewesen, hätte es im Idealfall gar nicht erst zu einem Informationssicherheitsvorfall kommen dürfen.

Damit schließt sich der Kreis: Die Vermeidung solcher Situationen liegt sowohl im Interesse der Unternehmen der Massivumformung als auch im Interesse des Gesetzgebers – und genau das ist das gemeinsame Ziel von NIS2.

Herr Kunde, wir danken Ihnen für das interessante Gespräch und die darin enthaltenen tiefgreifenden Informationen für die Unternehmen unserer Branche.

i

Karsten Kunde 1or2
Dipl. -Ing. Karsten Kunde
Sauerlandstraße 9
51688 Wipperfürth
Telefon: +49 2269 410
Mobil: +49 160 7411385
E-Mail: k.kunde@1or2.de
Internet: www.1or2.de