knooing

WHITE PAPER

Blind im Ernstfall?

Warum Unternehmen jetzt volle Transparenz über ihre IT-Applikationen brauchen – rechtlich und operativ

Cyberrisiko · NIS2-Compliance · IT-Transparenz

September 2026 · Ein White Paper von knooing

Inhalt

Executive Summary

Wer im Ernstfall nicht weiß, welche IT-Systeme im eigenen Unternehmen überhaupt laufen, kann sie weder schützen noch verteidigen.

Cyberangriffe auf deutsche Unternehmen haben ein Rekordniveau erreicht. Laut der Bitkom-Studie „Wirtschaftsschutz 2025“ waren 87 Prozent der Unternehmen in Deutschland innerhalb von zwölf Monaten von Datendiebstahl, Spionage oder Sabotage betroffen; der wirtschaftliche Gesamtschaden belief sich auf 289,2 Milliarden Euro. Gleichzeitig verschärft der Gesetzgeber mit dem NIS2-Umsetzungsgesetz (NIS2UmsuCG), das seit dem 6. Dezember 2025 ohne Übergangsfrist gilt, die Anforderungen an Risikomanagement, Meldepflichten und die persönliche Verantwortung der Geschäftsleitung.

In der Praxis entscheidet ein Faktor häufig darüber, ob ein Angriff ein kontrollierbarer Vorfall bleibt oder zur existenzbedrohenden Krise wird: ob ein Unternehmen im Ernstfall weiß, welche IT-Applikationen, Schnittstellen, Daten und Verträge überhaupt existieren und betroffen sind. Ohne aktuelle Übersicht werden Meldefristen von 24 Stunden verpasst, lässt sich der Angriff nicht eingrenzen, und die Nachweispflicht gegenüber Behörden, Kunden und Versicherern kann nicht erfüllt werden.

Dieses White Paper ordnet die Bedrohungslage ein, erläutert die rechtlichen Anforderungen an Unternehmen in Deutschland, beschreibt konkret, was im Ernstfall ohne IT-Applikationsübersicht passiert – und zeigt, wie die KI-gestützte IT-Management-Plattform knooing Unternehmen dabei unterstützt, diese Transparenz herzustellen und dauerhaft zu halten.

1. Die Bedrohungslage: Cyberangriffe auf Rekordniveau

Cyberangriffe sind für Unternehmen in Deutschland längst keine Ausnahmeerscheinung mehr, sondern statistische Gewissheit. Aktuelle Studien und Lageberichte zeichnen ein eindeutiges Bild:

87 %	**289,2 Mrd. €**	**241 Tage**
der Unternehmen in Deutschland waren betroffen von Datendiebstahl, Spionage oder Sabotage (Bitkom, 2025)	wirtschaftlicher Gesamtschaden durch Cyberangriffe in Deutschland (Bitkom, 2025)	durchschnittliche Zeit bis ein Sicherheitsvorfall erkannt und eingedämmt ist (IBM, weltweit, 2025)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt die Lage der IT-Sicherheit in Deutschland in seinem aktuellen Lagebericht als weiterhin „angespannt“ und benennt unzureichend geschützte Angriffsflächen als eine der zentralen Schwachstellen der deutschen Wirtschaft und Verwaltung. Angreifer – laut Bitkom zu je 46 Prozent der betroffenen Unternehmen Russland und China zugeordnet, ergänzt um zunehmend aktive ausländische Nachrichtendienste – nutzen dabei gezielt Schwachstellen in Software, Schnittstellen und Lieferketten aus.

Mit jeder zusätzlichen Applikation, jedem neuen SaaS-Tool und jeder neuen Schnittstelle wächst die Angriffsfläche eines Unternehmens. Gleichzeitig verschwimmt die Grenze zwischen einzelnen Systemen: Moderne IT-Landschaften bestehen aus Dutzenden bis Hunderten miteinander verbundener Applikationen,

Cloud-Diensten und Drittanbieter-Integrationen. Ein Angriff auf ein einziges, scheinbar unwichtiges Tool kann so zum Einfallstor für die gesamte Organisation werden.

2. Der blinde Fleck: Wenn niemand genau weiß, was eigentlich läuft

In der Beratungspraxis zeigt sich immer wieder dasselbe Muster: Viele Unternehmen – gerade im Mittelstand – verfügen über keine vollständige, aktuelle Übersicht ihrer eigenen IT-Applikationslandschaft. Historisch gewachsene Systeme, Fusionen und Übernahmen, dezentrale Beschaffung und der medienbruchbehaftete Wechsel zwischen Excel-Listen, Ticket-Systemen und dem Wissen einzelner Mitarbeitender führen dazu, dass niemand im Unternehmen eine verlässliche, vollständige Antwort auf die scheinbar einfache Frage geben kann: „Welche Applikationen, Services und Schnittstellen setzen wir eigentlich ein – und wer ist dafür verantwortlich?“

Schatten-IT als wachsendes Risiko

Ein wesentlicher Treiber dieses blinden Flecks ist Schatten-IT: Software und Cloud-Dienste, die Fachbereiche ohne Wissen oder Freigabe der IT-Abteilung beschaffen und nutzen. Der IBM „Cost of a Data Breach Report 2025“ zeigt exemplarisch, wie teuer mangelnde Governance werden kann: Ein hoher Anteil ungenehmigter, nicht überwachter KI-Anwendungen („Shadow AI“) erhöhte die durchschnittlichen Kosten eines Sicherheitsvorfalls im Schnitt um 670.000 US-Dollar – 63 Prozent der befragten Unternehmen gaben zudem an, über keine Governance-Richtlinien für KI-Werkzeuge zu verfügen. Das Muster lässt sich unmittelbar auf IT-Applikationen im Allgemeinen übertragen: Was nicht erfasst ist, wird auch nicht abgesichert, überwacht oder im Ernstfall berücksichtigt.

Die Konsequenz ist so einfach wie unbequem: Ein Unternehmen kann nur schützen, was es kennt. Jede nicht erfasste Applikation, jede vergessene Schnittstelle und jeder ungenutzte, aber noch aktive Account ist ein potenzielles Einfallstor – und gleichzeitig ein blinder Fleck im Ernstfall.

3. Gesetzliche Pflicht oder nur gute Praxis?

Die Frage, ob eine IT-Applikationsübersicht gesetzlich vorgeschrieben ist, lässt sich nicht mit einem einzigen Paragraphen beantworten – aber die Antwort ist im Ergebnis eindeutig: Ohne sie lassen sich die gesetzlichen Pflichten, die seit Ende 2025 für tausende Unternehmen in Deutschland gelten, faktisch nicht erfüllen.

Das NIS2-Umsetzungsgesetz (NIS2UmsuCG)

Das NIS2UmsuCG ist am 6. Dezember 2025 in Kraft getreten – ohne Übergangsfrist. Es betrifft schätzungsweise rund 29.500 Unternehmen in 18 Sektoren, sobald mindestens eine der folgenden Schwellen erreicht wird: 50 oder mehr Mitarbeitende oder mindestens 10 Millionen Euro Jahresumsatz in einem der erfassten Sektoren (u. a. Energie, Transport, Bankwesen, Gesundheit, Wasser, digitale Infrastruktur und öffentliche Verwaltung).

> **Zentrale Pflichten im Überblick**

> Registrierung beim BSI über das Meldeportal MUK: reguläre Frist war der 6. März 2026, eine Nachfrist läuft bis zum 31. Juli 2026 – wer sich noch nicht registriert hat, sollte dies umgehend nachholen.
>
> § 30 NIS2UmsuCG: zehn verpflichtende Maßnahmenbereiche des Risikomanagements, u. a. Risikoanalyse, Sicherheitskonzepte, Vorfallsbewältigung, Business-Continuity- und Backup-Management sowie Lieferkettensicherheit.
>
> § 32 NIS2UmsuCG: gestuftes Meldeverfahren bei Sicherheitsvorfällen – Erstmeldung innerhalb von 24 Stunden, Detailbericht innerhalb von 72 Stunden, Abschlussbericht innerhalb eines Monats.
>
> § 38 NIS2UmsuCG: persönliche Haftung der Geschäftsleitung für die Umsetzung angemessener Risikomanagementmaßnahmen.
>
> § 65 NIS2UmsuCG: Bußgelder von bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes für „besonders wichtige“ Einrichtungen, bis zu 7 Mio. € bzw. 1,4 % für „wichtige“ Einrichtungen.

Das Gesetz schreibt kein eigenständiges „IT-Applikationsinventar“ als isolierte Pflicht vor. Die in § 30 geforderten Risikomanagementmaßnahmen – Risikoanalyse, Sicherheitskonzepte, Vorfallsbewältigung – sind jedoch ohne eine strukturierte, aktuelle Erfassung aller IT-Systeme, Applikationen und Lieferanten praktisch nicht umsetzbar. Wer nicht weiß, welche Systeme im Unternehmen existieren, kann für sie keine Risikoanalyse durchführen, keine Sicherheitskonzepte definieren und im Vorfall nicht innerhalb von 24 Stunden melden, was genau betroffen ist. Für „besonders wichtige“ Einrichtungen kommt hinzu, dass sie gegenüber dem BSI bis Dezember 2028 in dreijährigem Turnus die Umsetzung dieser Maßnahmen nachweisen müssen – auch das setzt eine dokumentierte, auditfähige Übersicht voraus.

Weitere relevante Rahmenwerke

Für Unternehmen im Finanzsektor kommt zusätzlich der Digital Operational Resilience Act (DORA) hinzu, der ausdrücklich ein Verzeichnis aller IKT-Drittdienstleister verlangt. Und unabhängig von einer konkreten gesetzlichen Pflicht gilt: Normen wie ISO 27001 und der BSI IT-Grundschutz definieren ein vollständiges Asset-Management seit jeher als Kernbaustein eines funktionierenden Informationssicherheits-Managementsystems (ISMS). Auch Unternehmen außerhalb des unmittelbaren NIS2-Anwendungsbereichs geraten zunehmend indirekt unter Druck: Banken, Versicherer und größere Kunden verlangen im Rahmen von Due-Diligence-Prüfungen und für den Abschluss von Cyberversicherungen immer häufiger belastbare Nachweise über die eigene IT-Transparenz und -Sicherheit.

Rechtlicher Hinweis: Dieses White Paper bietet eine allgemeine Einordnung und ersetzt keine individuelle Rechtsberatung. Ob und in welchem Umfang ein Unternehmen unter das NIS2UmsuCG oder andere Regelwerke fällt, sollte im Einzelfall rechtlich geprüft werden.

4. Der Ernstfall: Was passiert ohne IT-Applikationsübersicht?

Ein Sicherheitsvorfall verläuft grundlegend anders, je nachdem, ob ein Unternehmen seine IT-Landschaft kennt oder nicht. Ohne aktuelle Applikationsübersicht entstehen typischerweise folgende Kettenreaktionen:

1. **Verzögerte Erkennung:** Ein kompromittiertes System wird oft erst spät erkannt, weil niemand einen vollständigen Überblick über alle laufenden Applikationen und deren Normalzustand hat – im

weltweiten Durchschnitt vergehen laut IBM 241 Tage bis zur Identifikation und Eindämmung eines Vorfalls.

2. **Unklare Angriffsfläche:** Ohne Wissen über bestehende Schnittstellen, Drittanbieter und Datenflüsse wird die Eindämmung zum Blindflug. Im schlimmsten Fall breitet sich ein Angriff unbemerkt über Verbindungen aus, deren Existenz niemand dokumentiert hatte.
3. **Nicht einhaltbare Meldefristen:** Die 24-Stunden-Erstmeldung an das BSI setzt voraus, sofort benennen zu können, was passiert ist und welche Systeme und Daten betroffen sind. Ohne Übersicht ist das faktisch nicht leistbar – mit entsprechendem Bußgeldrisiko und Vertrauensverlust bei der Aufsichtsbehörde.
4. **Fehlende Nachweisfähigkeit:** Im Audit oder auf Nachfrage von Behörden, Kunden oder Versicherern lässt sich nicht belegen, welche Sicherheitsmaßnahmen für welche Systeme überhaupt galten – mit direkten Folgen für Versicherungsschutz und Vertragsbeziehungen.
5. **Haftungsrisiko für die Geschäftsleitung:** Wer im Nachgang nicht nachweisen kann, ein angemessenes Risikomanagement – einschließlich Kenntnis der eigenen IT-Landschaft – betrieben zu haben, riskiert nach § 38 NIS2UmsuCG die persönliche Haftung der Geschäftsleitung.
6. **Höhere Wiederherstellungskosten:** Systeme, von deren Existenz IT und Geschäftsführung nichts wussten, werden beim Wiederaufbau übersehen oder erst spät entdeckt – ein häufiger Grund dafür, dass Unternehmen nach einem Angriff erneut kompromittiert werden.
7. **Reputationsschaden:** Kunden, Partner und Versicherer verlieren spürbar an Vertrauen, wenn im Nachgang eines Vorfalls öffentlich wird, dass ein Unternehmen schlicht nicht wusste, was in der eigenen IT lief.

5. Was eine belastbare IT-Applikationsübersicht leisten muss

Eine einmal jährlich aktualisierte Excel-Liste erfüllt weder den operativen noch den regulatorischen Anspruch an ein modernes IT-Inventar. Eine belastbare Übersicht muss:

- **Vollständig sein:** alle Applikationen, Services, Schnittstellen, Lizenzen und Verträge vollständig erfassen – einschließlich Schatten-IT.
- **Aktuell bleiben:** kontinuierlich und möglichst automatisiert aktuell gehalten werden, statt in periodischen, schnell veraltenden Erhebungen zu erstarren.
- **Prozesse verknüpfen:** jede Applikation mit Geschäftsprozessen, Verantwortlichkeiten und Verträgen verknüpfen – wer nutzt was, wofür, und mit welchen Daten?
- **Risiko bewerten:** jede Applikation nach Kritikalität, DSGVO-Relevanz und Lieferantenrisiko einordnen, statt IT und Risikomanagement getrennt zu betrachten.
- **Zentral zugänglich sein:** als zentrale, jederzeit abrufbare „Single Source of Truth“ für IT, Fachbereiche und Geschäftsführung dienen – statt im Kopf einzelner Mitarbeitender zu existieren.
- **Auditfähig sein:** lückenlose, exportierbare Nachweise für Behörden, Kunden und Versicherer liefern können.

6. Wie knooing hilft

knooing ist eine AI-native IT-Management-Plattform, die genau diese Transparenz herstellt – automatisiert, statt sie manuell zusammenzutragen. Statt verstreuter Excel-Listen, veralteter CMDB-Einträge und Wissen, das an einzelnen Personen hängt, schafft knooing eine zentrale, kontinuierlich aktuelle Wahrheit über die gesamte IT-Landschaft eines Unternehmens – für IT, Fachbereiche und Geschäftsführung gleichermaßen.

Die fünf Module im Überblick

- **IT Inventory & Capabilities –** Ein zentrales, KI-gestütztes Verzeichnis aller Applikationen, Services, Verträge und Lizenzen. Dokumente wie Verträge oder Lizenzunterlagen werden automatisiert per KI-Analyse ausgelesen, statt manuell in Tabellen gepflegt zu werden.
- **Risk & Compliance –** Kontinuierliches Monitoring von DSGVO-, DORA- und Lieferanten-Compliance, ein Risiko- und Compliance-Dashboard für Applikationen, Services und Lieferanten sowie Frühwarnungen bei kritischen Vertrags-, Datenschutz- oder Sicherheitsproblemen – ergänzt um lückenlose Audit-Logs aller Nutzer-, E-Mail- und Zugriffsaktivitäten.
- **Optimization Intelligence –** Automatische Erkennung funktionaler Überlappungen, redundanter Tools und ungenutzter Lizenzen – jede eingesparte, unnötige Applikation ist zugleich eine kleinere Angriffsfläche.
- **Demand Management –** Strukturierte, dokumentierte Software-Anfragen mit automatischem Portfolio-Abgleich – Schatten-IT wird durch einen transparenten, nachvollziehbaren Beschaffungsprozess ersetzt, statt zu entstehen.
- **Cost Intelligence –** Konsolidierte IT-Kostenallokation nach TBM-Logik (Technology Business Management) mit Prognosen – Transparenz über Kosten als Nebeneffekt der Transparenz über Applikationen.

Der Unterschied im Ernstfall

Der eigentliche Wert dieser Transparenz zeigt sich im Sicherheitsvorfall selbst: Statt tagelang Systeme, Verträge und Zuständigkeiten zusammenzusuchen, liefert knooing in Minuten eine belastbare Antwort auf die entscheidende Frage: „Welche Applikationen, Daten und Verträge sind betroffen – und wer ist verantwortlich?“ Das ist die Grundlage für eine fristgerechte Meldung nach § 32 NIS2UmsuCG, eine wirksame Eindämmung des Vorfalls und die Nachweisfähigkeit gegenüber BSI, Kunden und Versicherern.

7. Handlungsempfehlungen

Sieben konkrete Schritte, mit denen Unternehmen jetzt beginnen können:

1. **Bestandsaufnahme starten:** Vollständige Erhebung aller IT-Applikationen starten – einschließlich Schatten-IT, die nicht über die offizielle IT-Beschaffung läuft.
2. **Verantwortlichkeiten klären:** Für jede Applikation und jeden Datensatz eine verantwortliche Person (Owner) benennen.

3. **NIS2-Betroffenheit prüfen:** Die eigene NIS2-Betroffenheit prüfen und eine fehlende BSI-Registrierung umgehend nachholen (Nachfrist bis 31. Juli 2026).
4. **Risikomanagement dokumentieren:** Risikomanagement nach § 30 NIS2UmsuCG dokumentieren und direkt mit dem IT-Applikationsinventar verknüpfen.
5. **Ernstfall testen:** Ließen sich die Meldefristen von 24 Stunden, 72 Stunden und einem Monat mit der heutigen Übersicht tatsächlich einhalten? Den Incident-Response-Plan realistisch testen.
6. **Plattform statt Excel:** Statische, manuell gepflegte Inventare (Excel, veraltete CMDB) durch eine kontinuierlich aktuelle, zentrale Plattform ersetzen.
7. **Geschäftsführung einbinden:** Ein regelmäßiges Reporting an die Geschäftsführung etablieren, um das persönliche Haftungsrisiko nach § 38 NIS2UmsuCG nachweisbar zu minimieren.

Fazit

Cyberangriffe sind für Unternehmen in Deutschland keine abstrakte Gefahr mehr, sondern statistische Gewissheit – und ihre Folgen werden durch das NIS2-Umsetzungsgesetz erstmals unmittelbar zur persönlichen Angelegenheit der Geschäftsleitung. Ob ein Angriff zu einem kontrollierbaren Vorfall oder zu einer existenzbedrohenden Krise wird, entscheidet sich maßgeblich in den Minuten und Stunden danach – und damit an der Frage, ob ein Unternehmen weiß, was in seiner eigenen IT läuft.

Eine vollständige, aktuelle IT-Applikationsübersicht ist damit längst mehr als eine IT-Hygienemaßnahme: Sie ist die Grundlage, um gesetzliche Meldefristen einzuhalten, Haftungsrisiken zu begrenzen und im Ernstfall handlungsfähig zu bleiben. knooing schafft diese Transparenz nicht als einmaliges Projekt, sondern als lebendige, KI-gestützte Plattform, die mit dem Unternehmen mitwächst.

Über knooing

knooing ist eine AI-native IT-Management-Plattform, die Unternehmen volle Transparenz über ihre IT-Landschaft verschafft und datenbasierte IT-Entscheidungen in Minuten statt Wochen ermöglicht. Über fünf integrierte Module – IT Inventory & Capabilities, Risk & Compliance, Optimization Intelligence, Demand Management und Cost Intelligence – schafft knooing eine zentrale Wahrheit für IT, Fachbereiche und Geschäftsführung.
knooing ist SAP-Partner und wird von Unternehmenskunden wie Volvo Trucks Central Europe eingesetzt.

> **Kontakt**
>
> Sie möchten wissen, wie transparent Ihre eigene IT-Landschaft heute wirklich ist?
>
> knooing GmbH · www.knooing.com · hello@knooing.com
>
> Vereinbaren Sie eine unverbindliche Demo unter knooing.com.

Quellen

· Bitkom e. V.: Studie „Wirtschaftsschutz 2025“ – bitkom.org/Bitkom/Publikationen/Wirtschaftsschutz

· Bundesamt für Sicherheit in der Informationstechnik (BSI): „Die Lage der IT-Sicherheit in Deutschland 2025“ – bsi.bund.de/lagebericht

· IBM: „Cost of a Data Breach Report 2025“ – ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai

· NIS2-Umsetzungsgesetz (NIS2UmsuCG); IDW Knowledge Paper „Das NIS-2-Umsetzungsgesetz“, Stand 22.02.2026 – idw.de

· secjur GmbH: „NIS2 Umsetzung Deutschland: Gesetz, Fristen & Schritte“ – secjur.com/blog/nis2-umsetzung

· Docusnap GmbH: „NIS-2-Richtlinie: Anforderungen, Strafen & Pflichten“ – docusnap.com/en/it-documentation/nis2

· knooing: Plattform- und Feature-Übersicht – knooing.com/de/plattform, knooing.com/features

Alle Angaben ohne Gewähr. Stand: September 2026. Dieses Dokument stellt keine Rechtsberatung dar.