Die EU-Richtlinie NIS2 wird in einer Beitrags-Reihe behandelt. Den verschiedenen Aspekten dieses Themas widmen sich die folgenden Ausgaben:

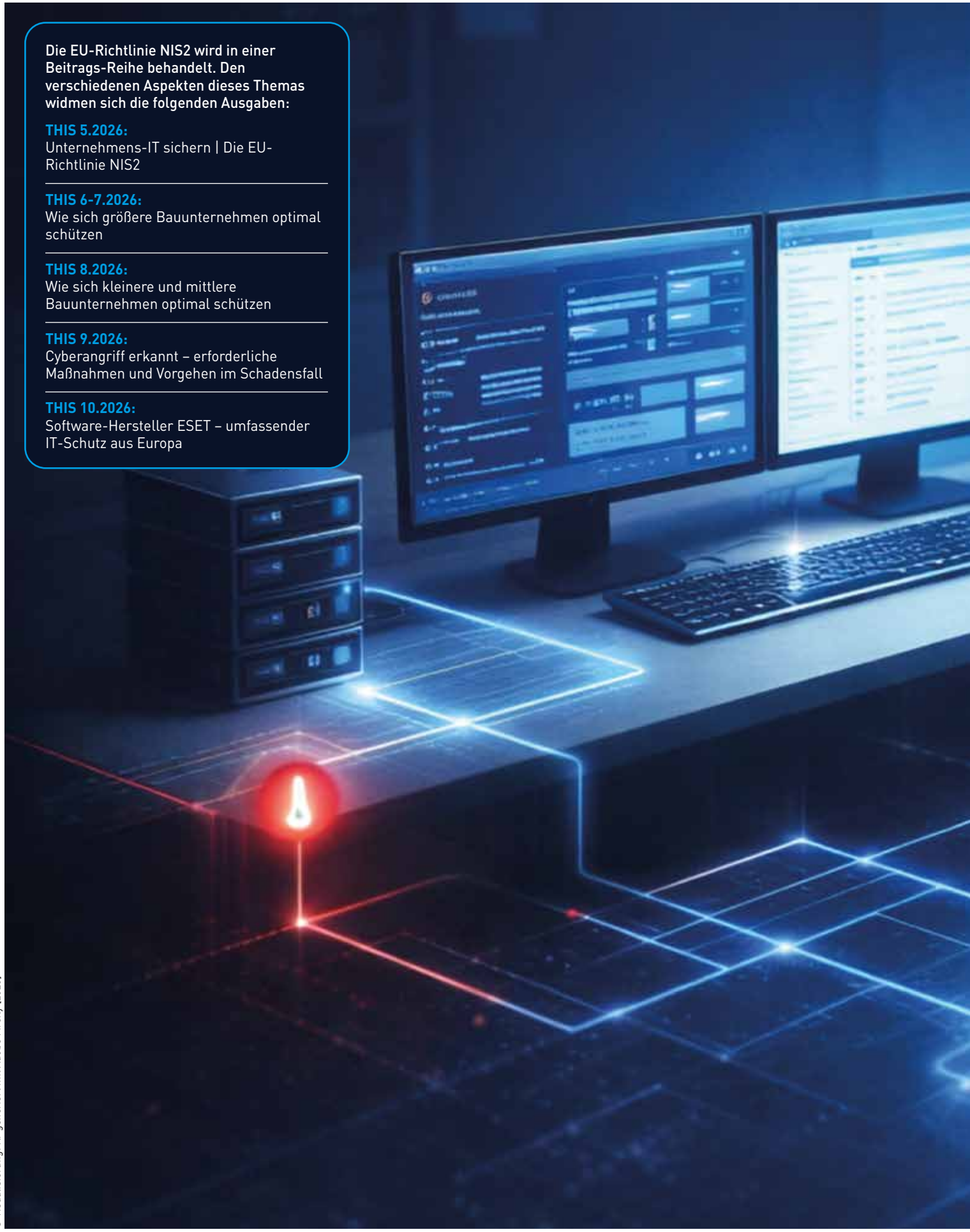
THIS 5.2026:
Unternehmens-IT sichern | Die EU-Richtlinie NIS2

THIS 6-7.2026:
Wie sich größere Bauunternehmen optimal schützen

THIS 8.2026:
Wie sich kleinere und mittlere Bauunternehmen optimal schützen

THIS 9.2026:
Cyberangriff erkannt – erforderliche Maßnahmen und Vorgehen im Schadensfall

THIS 10.2026:
Software-Hersteller ESET – umfassender IT-Schutz aus Europa



Unternehmens-IT sichern

Warum Cybersicherheit jetzt Chefsache ist

Im Dezember 2025 ist die NIS2-Richtlinie in Deutschland verbindlich in nationales Recht überführt worden. Damit rückt Cybersicherheit verstärkt in den Fokus der Unternehmensleitung und es entsteht Handlungsbedarf.

Eugen Schmitz

Montagmorgen, 7:30 Uhr. In einem mittelständischen Bauunternehmen beginnt der Arbeitstag – doch innerhalb weniger Minuten ist klar: Nichts funktioniert mehr. Die Projektplanung ist nicht erreichbar, Bestellungen können nicht ausgelöst werden, Rechnungen bleiben liegen. Stattdessen erscheinen auf den Bildschirmen nur noch Fehlermeldungen: Server nicht erreichbar. Datenbank offline. Was wie eine technische Störung beginnt, entpuppt sich schnell als massives Problem. Ohne Zugriff auf zentrale Daten stehen Baustellen still, Abläufe geraten ins Stocken, Entscheidungen können nicht getroffen werden. Jeder weitere Ausfall kostet Zeit – und Geld.

Solche Vorfälle sind längst keine Ausnahme mehr. Cyberangriffe treffen heute gezielt auch mittelständische Unternehmen. Gerade dort, wo Prozesse digital organisiert sind und Daten die Grundlage des Geschäfts bilden, kann ein Angriff den gesamten Betrieb lahmlegen. Mit der neuen EU-Richtlinie NIS2 rückt dieses Risiko stärker in den Fokus der Unternehmensleitung. Erstmals werden deutlich mehr Unternehmen verpflichtet, ihre IT-Sicherheit systematisch zu organisieren und Risiken aktiv entgegenzusteuern.

Seit dem 6. Dezember 2025 ist die Richtlinie in Deutschland verbindlich in nationales Recht umgesetzt. Unternehmen, die unter ihren Anwendungsbereich fallen, müssen sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren und erhebliche Sicherheitsvorfälle binnen 24 Stunden dem BSI melden. Für Geschäftsführer bedeutet das: Cybersicherheit ist keine reine IT-Frage mehr, sondern auch eine Frage der Unternehmensverantwortung.

ESET Deutschland GmbH
www.eset.com

© Visualisierung: KI-generiert mit Adobe Firefly [2026]

Die EU-Richtlinie NIS2

Pflichten erkennen, Risiken minimieren, Sicherheit stärken

Die EU-Richtlinie NIS2 erweitert den Kreis betroffener Unternehmen und verschärft die Anforderungen an Cybersicherheit. Für die Unternehmensleitung rücken klare Zuständigkeiten, Risikomanagement und Haftung stärker in den Fokus.

Eugen Schmitz

Die zweite europäische Richtlinie für Netz- und Informationssysteme, kurz „NIS2", soll die Cybersicherheit in der EU deutlich stärken – und sie betrifft künftig weit mehr Unternehmen als bisher. In Deutschland erfolgt die Umsetzung über das BSI-Gesetz unter Aufsicht des Bundesamt für Sicherheit in der Informationstechnik. Cybersicherheit wird damit nicht länger ein optionales IT-Thema, sondern ein fester Bestandteil verantwortungsvoller Unternehmensführung und rückt zunehmend in den Fokus der Leitungsebene.

NIS2 wird verbindlich: Warum Unternehmen jetzt handeln müssen

Unabhängig von NIS2 gilt: Unternehmen müssen ihre Risiken kennen und angemessen steuern. Dazu gehört auch der Schutz der eigenen IT-Systeme. Wer hier untätig bleibt, handelt nicht nur wirtschaftlich riskant, sondern setzt sich auch erheblichen rechtlichen Risiken aus.

Hinzu kommt der zunehmende Druck aus der Praxis. Auftraggeber, Geschäftspartnerinnen und Versicherer orientieren sich bereits an den kommenden Anforde-

rungen und geben diese entlang der Lieferkette weiter. Wer heute in Projekten tätig ist, die über nationale Grenzen hinausgehen, wird mit entsprechenden Erwartungen bereits konfrontiert.
Die entscheidende Frage ist daher nicht, ob NIS2 formal schon gilt – sondern ob die eigene IT einem gezielten Angriff standhalten würde.

Strukturen schaffen statt Einzelmaßnahmen
Viele Unternehmen reagieren auf Cyberrisiken mit einzelnen Maßnahmen: neue Software, zusätzliche Sicherheitslösungen oder externe Dienstleistungen. Was dabei oft fehlt, ist ein klarer Gesamtansatz.
Cybersicherheit beginnt mit der Frage: Welche Systeme sind für unseren Betrieb wirklich kritisch? In Bauunternehmen sind das häufig Projektplattformen, Kalkulationssoftware, E-Mail-Systeme, Dokumentenablagen oder ERP-Lösungen. Fällt eines dieser Systeme aus, hat das direkte Auswirkungen auf Abläufe, Termine und Zahlungsprozesse.
Auf dieser Basis müssen Zuständigkeiten eindeutig geklärt werden. Wer trägt die Verantwortung für die Cybersicherheit im Unternehmen? Wer entscheidet im Ernstfall? Und wer übernimmt die Koordination, wenn schnelle Maßnahmen erforderlich sind? Ohne diese Klarheit entsteht im Krisenfall Unsicherheit – und die kostet wertvolle Zeit.
Ebenso entscheidend ist eine belastbare Bewertung der tatsächlichen Risiken. Welche Systeme sind besonders anfällig? Welche Daten sind unverzichtbar? Und welche konkreten Folgen hätte ein Ausfall? Cybersicherheit wird erst dann wirksam, wenn sie sich an den tatsächlichen Geschäftsprozessen orientiert.

Technik: Weniger ist mehr – wenn es richtig gemacht ist
Auf technischer Ebene geht es nicht darum, möglichst viele Lösungen einzusetzen, sondern die richtigen – konsequent und zuverlässig. Ein zentraler Punkt ist die Aktualität der Systeme. Veraltete Software gehört zu einem der häufigsten Angriffspunkte. Regelmäßige Updates sind daher keine Kür, sondern Pflicht. Entscheidend ist dabei nicht das einmalige Erreichen eines Schutzniveaus oder die Anschaffung einzelner Produkte, sondern deren kontinuierliche Überprüfung und Anpassung. Nur so lässt sich sicherstellen, dass der Schutz auch unter veränderten Bedingungen wirksam bleibt.
Ebenso entscheidend sind klar geregelte Zugriffsrechte. Nicht alle Mitarbeitenden benötigen Zugriff auf alle Systeme oder Daten. Wer hier sauber trennt, reduziert das Risiko erheblich. In der Praxis entstehen Schwachstellen häufig dort, wo Berechtigungen über längere Zeit anwachsen – etwa bei Auszubildenden oder Mitarbeitenden, die mehrere Abteilungen durchlaufen und deren Zugriffe anschließend nicht konsequent zurückgenommen werden.
Ein weiterer Schlüsselbereich ist die Datensicherung. Backups müssen vorhanden sein – und vor allem regelmäßig getestet und im Ernstfall verfügbar sein. Dann entscheidet nämlich genau diese Verfügbarkeit darüber, ob ein Unternehmen innerhalb von Stunden wieder arbeitsfähig ist oder für Tage stillsteht.
Auch Endgeräte spielen eine größere Rolle, als oft angenommen wird. Laptops, Smartphones und mobile Geräte sind häufig das Einfallstor für Angriffe – insbesondere dann, wenn sie außerhalb des Unternehmensnetzwerks genutzt werden.

Typische Schwachstellen
In der Praxis beruhen erfolgreiche Angriffe selten auf hochkomplexen Methoden, sondern meist auf bekannten Schwachstellen in Systemen und Organisation. Dazu zählen vor allem ungepatchte Betriebssysteme und Anwendungen – also Software, bei der Sicherheitslücken nicht durch Updates und Patches geschlossen wurden. Wichtig ist: Aktualisierungen sollten als kontinuierlicher Prozess fest etabliert sein. Ebenso kritisch sind zu weit gefasste Berechtigungen und fehlende Netzwerksegmentierung, wodurch sich Angriffe im Unternehmen leicht ausbreiten können.
Auch beim Zugriffsschutz gibt es oft Lücken: Fehlende Mehr-Faktor-Authentifizierung – besonders bei externen Zugängen – sowie schlecht gesicherte Remote-Verbindungen zählen zu den häufigsten Einfallstoren. Hinzu kommen Backups, die zwar existieren, im Ernstfall aber nicht funktionieren, weil sie nie getestet wurden.
Ein weiterer Schwachpunkt ist die fehlende Protokollierung und Auswertung sicherheitsrelevanter Ereignisse. Ohne Transparenz bleiben Angriffe oft lange unbemerkt.
Die zentrale Erkenntnis: Die meisten Vorfälle entstehen nicht durch fehlende Technik, sondern durch unzureichend umgesetzte Standards. Eine externe Überprüfung durch Spezialisten hilft, Schwachstellen zu erkennen und realistisch zu bewerten.

Kleine Unternehmen: Gleiches Risiko, andere Ausgangslage

Gerade kleinere Unternehmen unterschätzen häufig ihr eigenes Risiko. Die Annahme, dass man selbst für Angriffe nicht interessant sei, ist weit verbreitet – und in der Praxis falsch.

Angriffe erfolgen heute oft automatisiert und treffen gezielt dort, wo Systeme leicht zugänglich sind. Kleinere Strukturen sind daher häufig leichter angreifbar und deshalb gefährdeter.

Gleichzeitig ist die Abhängigkeit von funktionierender IT meist genauso hoch wie in größeren Unternehmen. Fällt ein zentrales System aus, steht oft der gesamte Betrieb still.

Die gute Nachricht: Der Einstieg in eine wirksame Cybersicherheit ist überschaubar. Klar definierte Maßnahmen wie regelmäßige Updates, funktionierende Backups, eingeschränkte Benutzerrechte und sensibilisierte Mitarbeitende können das Risiko deutlich reduzieren.

Entscheidend ist nicht die Größe des Unternehmens, sondern die Rolle, die Cybersicherheit im täglichen Betrieb spielt.

Der Ernstfall: vorbereitet sein statt improvisieren

Kommt es zu einem Sicherheitsvorfall, entscheidet die Vorbereitung über den Schaden. Unternehmen sollten nicht erst im Ernstfall überlegen, wie sie reagieren.

Zu den wichtigsten ersten Maßnahmen gehört es, betroffene Systeme schnell zu isolieren, um eine weitere Ausbreitung zu verhindern. Parallel muss geklärt werden, welche Systeme betroffen sind und wie der Betrieb stabilisiert werden kann.

Spezialisierte Cybersicherheitsdienstleister sind dabei häufig unverzichtbar. Viele Unternehmen verfügen nicht über die notwendigen Ressourcen, um komplexe Vorfälle eigenständig zu bewältigen.

Hinzu kommen Meldepflichten, die innerhalb kurzer Fristen erfüllt werden müssen. Ohne vorbereitete Abläufe kann das schnell zur zusätzlichen Belastung werden.

Ebenso entscheidend ist die Kommunikation – intern wie extern. Unklare oder verspätete Informationen können den Schaden erheblich vergrößern.

Cybersicherheit ist ein Prozess

Cybersicherheit lässt sich nicht einmalig „einführen". Die Bedrohungslage entwickelt sich kontinuierlich weiter – und damit auch die Anforderungen.

Unternehmen sollten ihre Sicherheitsmaßnahmen regelmäßig überprüfen und an veränderte Bedrohungslagen anpassen. Dazu gehören klare Prozesse, definierte Zuständigkeiten und wiederkehrende Tests.

Ziel ist keine absolute Sicherheit – die gibt es nicht. Entscheidend ist eine IT-Struktur, die stabil funktioniert und auch im Ernstfall beherrschbar bleibt.

Haftung: Nichtstun wird zum Risiko

Cybersicherheit ist längst auch eine Frage der Unternehmensverantwortung. Geschäftsleiterinnen und -leiter sind verpflichtet, ihre Unternehmen so zu organisieren, dass vorhersehbare Risiken beherrscht werden – dazu gehört heute ausdrücklich auch die IT.

Kommt es zu einem Vorfall und zeigt sich, dass grundlegende Maßnahmen unterlassen wurden – etwa fehlende Backups, unzureichende Zugriffskontrollen oder veraltete Systeme –, kann dies als Organisationsver-

Warum jetzt gehandelt werden muss

Die Anforderungen an die Cybersicherheit ergeben sich auch ohne vollständige nationale Umsetzung bereits aus allgemeinen Organisationsanforderungen. Geschäftsleitungen sind verpflichtet, Risiken für das Unternehmen zu erkennen und angemessen zu steuern – dazu gehört ausdrücklich auch die Absicherung der IT-Systeme.

In der Praxis wird dabei nicht entscheidend sein, ob eine konkrete Vorschrift formal bereits gilt, sondern ob ein Unternehmen nachweisbar dem Stand der Technik entspricht. Dieser Maßstab ergibt sich unter anderem aus § 93 AktG (Sorgfaltspflicht der Geschäftsleitung), § 43 GmbHG sowie aus den Grundsätzen ordnungsgemäßer Unternehmensorganisation.

Gleichzeitig verschiebt sich der Druck aus der Praxis. Auftraggebende, Versichernde und geschäftliche Kontakte orientieren sich zunehmend an den erwarteten NIS2-Standards und verlangen entsprechende Nachweise von ihren Auftragnehmenden, Zulieferern und Dienstleistenden. Auch Unternehmen, die formal nicht unter die NIS2-Regelung fallen, werden damit faktisch in die Anforderungen einbezogen. Die Unterscheidung zwischen direkt und indirekt betroffenen Unternehmen verliert in der Praxis zunehmend an Bedeutung.

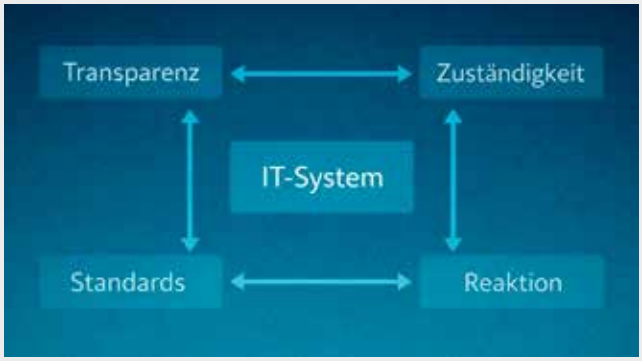
Die Konsequenz: Wer bekannte Risiken nicht adressiert, handelt nicht nur wirtschaftlich fahrlässig, sondern bewegt sich zunehmend in einem haftungsrelevanten Bereich.

Cybersicherheit systematisch umsetzen

Cybersicherheit entsteht nicht durch einzelne Maßnahmen, sondern durch eine strukturierte und nachvollziehbare Organisation. Entscheidend ist, dass Sicherheitsanforderungen systematisch im Unternehmen verankert sind und im Alltag funktionieren.

- **Transparenz:** Kritische Systeme, Daten und Abhängigkeiten sind bekannt und nachvollziehbar erfasst. Nur so lassen sich Risiken realistisch bewerten und priorisieren.
- **Klare Zuständigkeiten:** Es ist festgelegt, wer für Cybersicherheit verantwortlich ist, wer Entscheidungen trifft und wie im Ernstfall vorzugehen ist. Fehlende Verantwortlichkeiten führen in der Praxis regelmäßig zu Verzögerungen und erhöhen das Schadensrisiko.
- **Konsequent umgesetzte Standards:** Dazu zählen geregeltes Patch-Management, kontrollierte Zugriffsrechte, abgesicherte externe Zugänge sowie regelmäßig geprüfte Datensicherungen.
- **Reaktionsfähigkeit:** Sicherheitsrelevante Ereignisse werden erkannt, bewertet und dokumentiert. Vorfälle lassen sich strukturiert bearbeiten.

Cybersicherheit ist dann wirksam, wenn sie organisatorisch verankert ist – und nicht nur aus Einzelmaßnahmen besteht.



schulden gewertet werden. Entsprechende Schutzmechanismen und Softwarelösungen wie beispielsweise ESET sind heute breit verfügbar, wirtschaftlich vertretbar und gelten als Stand der Technik. Sie werden jedoch in vielen Unternehmen noch nicht konsequent genutzt.

Entscheidend ist dabei weniger, ob NIS2 bereits formal umgesetzt ist, sondern viel mehr, ob ein Unternehmen angemessen auf erkennbare Risiken reagiert hat. Wer hier untätig bleibt, geht ein doppeltes Risiko ein: wirtschaftlich – und persönlich.

In den Ausgaben 6-7.2026 und 8.2026 stellt THIS strukturierte Ansätze und praxisnahe Konzepte vor, mit denen sich sowohl größere als auch kleinere Unternehmen systematisch gegen Cyberrisiken absichern können.

ESET Deutschland GmbH
www.eset.com

„Wer sich nicht informiert, setzt sich einem erhöhten Haftungsrisiko aus“

Die Ansprüche an die unternehmenseigene Cybersicherheit steigen

Die THIS sprach mit Rechtsanwalt Dr. Jens Eckhardt über das BSI-Gesetz, die deutsche Umsetzung der EU-Richtlinie NIS2, und über die wachsende Verantwortung von Unternehmerinnen und Unternehmern.

THIS: Was ist eigentlich das Ziel hinter der NIS2-Richtlinie und dem BSI-Gesetz?

Dr. Jens Eckhardt: Zur Einordnung: NIS steht für Netzwerk- und Informationssicherheit. Die NIS2-Richtlinie ist nicht die erste Regelung dieser Art, sondern baut auf bestehenden Vorgängerregelungen auf, die sich vor allem auf den Schutz kritischer Infrastrukturen konzentriert haben. Mit der Zeit hat sich jedoch gezeigt, dass sich die Bedrohungslage deutlich verändert hat, insbesondere durch steigende Cyberrisiken. Vor diesem Hintergrund verfolgt NIS2 einen breiteren und moderneren Ansatz.

Der Fokus liegt nicht mehr nur darauf, Angriffe zu verhindern, sondern auch darauf, wie gut ein Unternehmen

mit einem Angriff umgehen kann. Es geht um Resilienz. In der Cybersicherheit gilt längst die Erkenntnis, dass nicht die Frage ist, ob ein Angriff stattfindet, sondern wann. Entscheidend ist daher, wie stark die Auswirkungen sind und wie schnell ein Unternehmen wieder zum Normalbetrieb zurückkehren kann.
Zusätzlich werden Risiken aus der Lieferkette und durch Drittanbieter stärker berücksichtigt und der Anwendungsbereich wurde deutlich erweitert. Es geht nicht mehr nur um klassische kritische Infrastrukturen, sondern auch um sogenannte wichtige und besonders wichtige Einrichtungen, also Unternehmen, die für Gesellschaft und Wirtschaft eine besondere Bedeutung haben.

THIS: Wie verhält sich das zur deutschen Gesetzgebung?

Dr. Jens Eckhardt: Die NIS2 ist eine EU-Richtlinie. Das bedeutet, sie gilt nicht unmittelbar, sondern muss in nationales Recht umgesetzt werden. In Deutschland erfolgte diese Umsetzung über das BSI-Gesetz mit Geltung seit dem 6. Dezember 2025. Die eigentlichen materiellen Regelungen zur NIS2 finden sich dort ab den entsprechenden Vorschriften im mittleren Teil des Gesetzes.
In der öffentlichen Kommunikation spricht man oft von NIS2, weil das griffiger ist. Rechtlich verbindlich ist in Deutschland jedoch das BSI-Gesetz. Es setzt die Vorgaben der Richtlinie um und konkretisiert sie.

THIS: Sind NIS2 und BSI-Gesetz identisch oder gibt es Unterschiede?

Dr. Jens Eckhardt: Die Richtlinie gibt den Rahmen vor, das nationale Gesetz verleiht diesem Rahmen Geltung. Der Gesetzgeber ist verpflichtet, entsprechende Regelungen zu schaffen. In der Praxis bedeutet das, dass es gewisse Unterschiede im Wortlaut und im Detailverständnis geben kann.
Zudem haben alle EU-Mitgliedstaaten die Richtlinie eigenständig umgesetzt. Dabei sind bereits jetzt Unterschiede erkennbar. Diese Divergenzen werden in der Praxis noch eine Rolle spielen, insbesondere für Unternehmen, die in mehreren Ländern tätig sind.

THIS: Wer ist konkret verpflichtet?

Dr. Jens Eckhardt: Das BSI-Gesetz unterscheidet zwischen sogenannten besonders wichtigen Einrichtungen und wichtigen Einrichtungen. Die früheren kritischen Infrastrukturen fallen weiterhin unter die Regulierung, sind aber jetzt ein Unterfall der besonders wichtigen Einrichtungen.
Für die konkreten Pflichten macht diese Differenzierung in der Praxis nur einen begrenzten Unterschied. Sie wirkt sich vor allem auf den Bußgeldrahmen aus, weniger auf die inhaltlichen Anforderungen.

THIS: Wie wird entschieden, ob ein Unternehmen darunterfällt?

Dr. Jens Eckhardt: Die Einordnung erfolgt im Wesentlichen über zwei Kriterien. Zum einen muss das Unternehmen in einem bestimmten, im Gesetz definierten Sektor tätig sein. Zum anderen muss es eine bestimmte Größe erreichen, die anhand von Mitarbeitendenzahlen oder wirtschaftlichen Kennzahlen wie Umsatz oder Bilanzsumme bestimmt wird. Nur wenn beide Voraussetzungen erfüllt sind, fällt ein Unternehmen in den Anwendungsbereich.
Daneben gibt es aber auch Unternehmen, die unabhängig von ihrer Größe verpflichtet sind, etwa bestimmte Anbieter im Bereich digitaler Infrastruktur.

THIS: Das Gesetz gilt ohne Übergangsfrist. Warum?

Dr. Jens Eckhardt: Der Gesetzgeber argumentiert, dass die Wirtschaft seit Jahren wusste, dass entsprechende Regelungen kommen würden. Spätestens mit dem Inkrafttreten der Richtlinie war klar, dass eine Umsetzung erfolgen wird. Daraus wird abgeleitet, dass ausreichend Zeit bestand, sich vorzubereiten.
In der Praxis ist diese Argumentation durchaus kritisch zu sehen, weil sich die nationale Umsetzung verzögert hat. Wenn schon der Staat statt der vorgesehenen Umsetzungsfrist von knapp zwei Jahren die doppelte Zeit gebraucht hat, scheint das Thema doch nicht ganz so trivial zu sein.

THIS: Wie sollen Unternehmen das schaffen?

Dr. Jens Eckhardt: Die Unternehmen fangen ja nicht bei Null an. Cybersicherheit und Risikomanagement waren schon zuvor Teil der allgemeinen Pflichten der Geschäftsführung. Unternehmen, die sich damit bislang nicht beschäftigt haben, haben auch schon vor Inkrafttreten der neuen Regelungen gegen bestehende Pflichten verstoßen.
In vielen Fällen geht es daher weniger um einen kompletten Neustart, sondern um die Anpassung und Konkretisierung bestehender Systeme. Allerdings gab es auch Unsicherheiten, insbesondere bei der Frage, welche Unternehmen konkret unter die neuen Regelungen fallen.

THIS: Welche Pflichten ergeben sich konkret aus dem Gesetz?

Dr. Jens Eckhardt: Zunächst gibt es eine Registrierungspflicht. Unternehmen, die unter das Gesetz fallen, mussten sich beim Bundesamt für Sicherheit in der Informationstechnik registrieren. Dabei geht es nicht darum, die Umsetzung der Maßnahmen nachzuweisen, sondern lediglich darum, dem BSI mitzuteilen, dass man in den Anwendungsbereich fällt.
Zweitens besteht eine Pflicht zum Risikomanagement. Unternehmen müssen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen, um die Sicherheit ihrer IT-Systeme zu gewährleisten. Dabei ist der Stand der Technik maßgeblich. Neu ist insbesondere die stärkere Betonung der Resilienz, also der Fähigkeit, auch nach einem Angriff schnell wieder arbeitsfähig zu sein.
Drittens gibt es Meldepflichten bei Sicherheitsvorfällen. Bei erheblichen Vorfällen muss innerhalb von 24

Stunden eine erste Meldung erfolgen, nach 72 Stunden eine vertiefte Meldung und schließlich nach einem Monat ein Abschlussbericht.
Viertens besteht eine Pflicht zur Schulung der Geschäftsleitung. Die Geschäftsführung muss sich aktiv Wissen im Bereich der IT-Sicherheit aneignen, um Risiken erkennen und bewerten zu können.

THIS: Was bedeutet das für Geschäftsführer konkret?

Dr. Jens Eckhardt: Der Zusammenhang ist relativ einfach: Wer mehr weiß, muss auch mehr tun. Mit steigender Kenntnis steigt die Verantwortung. Wer sich nicht informiert oder vorhandenes Wissen nicht nutzt, setzt sich einem erhöhten Haftungsrisiko aus.

THIS: Kann man diese Verantwortung delegieren?

Dr. Jens Eckhardt: Eine vollständige haftungsbefreiende Delegation gab es auch bisher schon nicht und gibt es weiterhin nicht. Die Geschäftsleitung bleibt in der Verantwortung, auch wenn Aufgaben intern verteilt werden.

THIS: Wie ist das bei mehreren Geschäftsführern?

Dr. Jens Eckhardt: Auch hier gilt: Es besteht eine gemeinsame Verantwortung. Zuständigkeiten können zwar intern verteilt werden, aber das entbindet die anderen Mitglieder der Geschäftsleitung nicht vollständig. Neu ist vor allem, dass alle Mitglieder ein gewisses Mindestmaß an Verständnis für Cyberrisiken entwickeln müssen.
Das bedeutet nicht, dass jede Person zum IT-Experten werden muss. Aber es reicht nicht mehr aus, sich vollständig auf einzelne im Unternehmen Zuständige zu verlassen. Die Geschäftsleitung insgesamt muss in der Lage sein, Risiken zu erkennen und Entscheidungen nachzuvollziehen.

THIS: Müssen Unternehmen ihre gesamte Lieferkette absichern?

Dr. Jens Eckhardt: Wichtig ist: Es geht nicht um die klassische Lieferkette eines Produkts, sondern um die IT-bezogene Lieferkette. Relevant sind also insbesondere Dienstleistende und Anbieter, die Einfluss auf die IT-Infrastruktur eines Unternehmens haben.
Ein Unternehmen muss sicherstellen, dass diese IT-bezogenen Abhängigkeiten keine Sicherheitsrisiken darstellen. Das bedeutet aber nicht, dass jeder Lieferant eines physischen Produkts automatisch in diese Betrachtung einbezogen wird.

THIS: Wie ist das bei digitalen Plattformen oder gemeinsamen Arbeitsumgebungen?

Dr. Jens Eckhardt: Entscheidend ist, wer die Plattform nutzt oder betreibt. Dieses Unternehmen muss sicherstellen, dass die eingesetzten Systeme so abgesichert sind, dass externe Zugriffe nicht zu einem Risiko für die eigene IT-Infrastruktur werden. Das betrifft beispielsweise Zugangskontrollen und die Verarbeitung eingehender Daten.

© Eckhardt Rechtsanwälte Partnerschaft mbB

Rechtsanwalt Dr. Jens Eckhardt ist Fachanwalt für Informationstechnologie-Recht, Datenschutz-Auditor (TÜV) und IT-Compliance Manager (TÜV). Seit 2001 berät er bundesweit nationale und internationale Unternehmen zu den Themen Datenschutz, Informationstechnologie, Telekommunikation und Marketing – www.pitc-legal.de

THIS: Was passiert bei international tätigen Unternehmen?

Dr. Jens Eckhardt: Das ist aktuell eine der komplexesten Fragen. Grundsätzlich gilt das Territorialprinzip, also das Recht des Landes, in dem das Unternehmen ansässig ist. In der Praxis wird es jedoch kompliziert, weil die einzelnen Mitgliedstaaten die Richtlinie unterschiedlich umgesetzt haben.
Ein wesentlicher Kritikpunkt ist, dass es sich um eine Richtlinie und nicht um eine Verordnung handelt. Eine Verordnung hätte zu einheitlichem Recht in der gesamten EU geführt. Durch die Richtlinie entstehen dagegen Unterschiede, die für Unternehmen mit grenzüberschreitender Tätigkeit zu erheblicher Komplexität führen.

THIS: Welche Rolle spielt das Gesetz bei Bauprojekten oder Ausschreibungen?

Dr. Jens Eckhardt: Das Gesetz regelt nicht das Bauprodukt, sondern ist auf das Unternehmen und dessen Handlungsfähigkeit ausgerichtet. Es geht also nicht um die Sicherheit des errichteten Bauwerks, sondern um die Cybersicherheit des Unternehmens, das die Leistungen erbringt.

THIS: Was bedeutet das für Arbeitsgemeinschaften oder Subunternehmer?

Dr. Jens Eckhardt: Entscheidend ist, ob die jeweilige Organisation selbst unter das Gesetz fällt. Wenn das der Fall ist, muss sie die entsprechenden Anforderungen erfüllen. Subunternehmen sind nicht automatisch verpflichtet, es sei denn, sie fallen selbst unter die Regelungen.
Allerdings muss ein verpflichtetes Unternehmen sicherstellen, dass seine eigene IT-Infrastruktur nicht durch Dritte gefährdet wird. Das kann in der Praxis dazu führen, dass Anforderungen an Partner gestellt werden, auch wenn diese selbst nicht unmittelbar gesetzlich verpflichtet sind. □