kaspersky cybersecurity true to business

Kaspersky – Ihr verlässlicher Partner für die NIS-2-Umsetzung

Die **NIS-2-Richtlinie der Europäischen Union**[1] ist ein wichtiger Pfeiler der europäischen Cybersicherheits-Gesetzgebung. Sie verfolgt das Ziel, die Cybersicherheit in Europa weiter zu erhöhen und ein möglichst einheitliches Niveau sicherzustellen. In Deutschland wurde die Richtlinie durch das **Gesetz zur Umsetzung der NIS-2-Richtlinie** in nationales Recht umgesetzt. Durch das NIS-2-Umsetzungsgesetz wurden mehrere Gesetze, darunter das BSI-Gesetz, geändert. Seit dem 6. Dezember 2025 ist das neue Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen in Kraft. Das BSI-Gesetz definiert die Compliance-Anforderungen für alle betroffenen Unternehmen.

Wer ist von NIS 2 betroffen?

Betroffen sind Einrichtungen, die im BSI-Gesetz (BSIG) in „wichtige" und „besonders wichtige Einrichtung" untergliedert werden (vgl. §§ 28 und 29 BSIG).

Hierzu gehören:

- **Einrichtungen aus bestimmten Sektoren** (vgl. Anlagen 1 und 2 des BSIG) in Abhängigkeit von Mitarbeiterzahl, Umsatz und Jahresbilanzsumme
- **Betreiber kritischer Anlagen** (KRITIS-Betreiber)
- **Einrichtungen der Bundesverwaltung**

Darüber hinaus gilt das BSIG für sämtliche Anbieter von qualifizierten Vertrauensdiensten, Top Level Domain Name Registries oder DNS-Diensteanbieter – unabhängig von ihrer Größe. Das **Bundesamt für Sicherheit in der Informationstechnik** ist NIS-2-Aufsichtsbehörde und bietet eine Online-Betroffenheitsprüfung an.

Wesentliche Compliance Pflichten

Wichtige und besonders wichtige Einrichtungen müssen umfassende Risikomanagement- und Cybersicherheitsmaßnahmen umsetzen. Verantwortlich für die Umsetzung und Überwachung ist die Geschäftsleitung. Werden diese Pflichten verletzt, entstehen Haftungsrisiken und es drohen Bußgelder. **Die wesentlichen Pflichten sind:**

- **Risikomanagement & Technische Maßnahmen:** Betroffene Einrichtungen müssen geeignete, wirksame und verhältnismäßige Risikomanagementmaßnahmen implementieren und dokumentieren. Dazu zählen unter anderem IT-Sicherheitskonzepte, Zugriffskontrollen, Backup-Management und Wiederherstellung nach einem Notfall, Krisenmanagement, sowie Sicherheitsvorkehrungen für die Lieferkette.
- **Meldepflichten:** Erhebliche Sicherheitsvorfälle müssen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet werden. Dies erfordert eine Frühwarnung innerhalb von 24 Stunden, eine detaillierte Meldung binnen 72 Stunden sowie einen Abschlussbericht.
- **Registrierungspflicht:** Betroffene Einrichtungen müssen sich beim BSI registrieren und dabei u.a. Kontaktdaten und IP-Adressbereiche angeben.
- **Leitungsorgane & Schulung:** Die Geschäftsleitung muss die Risikomanagementmaßnahmen genehmigen, deren Umsetzung überwachen und sich regelmäßig fortbilden. Zudem sind Schulungsangebote für die Mitarbeitenden sicherzustellen.

Als Aufsichtsbehörde bietet das BSI strukturierte Informationen zur NIS-2-Risikoanalyse, zur sicheren Lieferkette, zur Geschäftsleitungsschulung sowie umfassende FAQs an.

[1] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie); https://eur-lex.europa.eu/eli/dir/2022/2555

Kaspersky – als besonders wichtige Einrichtung beim BSI registriert

Kaspersky ist seit März 2026 gemäß BSI-Gesetz als **Managed Security Service Provider (MSSP)** beim **Bundesamt für Sicherheit in der Informationstechnik (BSI)** als **besonders wichtige Einrichtung** registriert. Die Registrierung gilt für die gesamte EU. Bereits in der Phase, in der NIS 2 in Europa auf den Weg gebracht wurde, hat Kaspersky ein **umfassendes Compliance-Framework** implementiert. Das Unternehmen hat dazu seine Prozesse, Dokumentationen und Risikomanagementmethoden proaktiv auf die heute geltenden Anforderungen ausgerichtet. Auf Basis dieser Erfahrung unterstützt Kaspersky Unternehmen in Deutschland und Österreich dabei, ihre NIS-2-Pflichten effizient zu erfüllen sowie ihre Cybersicherheit und Resilienz nachhaltig zu steigern.

Wie die Lösungen und Services von Kaspersky Unternehmen unterstützen

Kaspersky unterstützt Unternehmen mit einer breiten Palette an technischen Lösungen und Services, abgestimmt auf ihre individuellen Anforderungen:

Extended Detection and Response (XDR): XDR ist eine technische Lösung, die Sicherheitsdaten aus mehreren Quellen in der IT-Umgebung eines Unternehmens sammelt und analysiert, um Bedrohungen frühzeitig zu erkennen und effektiver auf Vorfälle zu reagieren. Während sich Endpoint Detection and Response (EDR) auf die Endgeräte-Ebene konzentriert, erweitert XDR diesen Blickwinkel. Kaspersky Next XDR Optimum baut auf wichtigen EDR-Funktionen wie Ursachenanalyse oder IoC-Untersuchung auf und verstärkt Ihre Sicherheit durch mehr Transparenz und automatisierte Reaktionsfunktionen. Für Unternehmen ist die Lösung fokussiert und einfach zu verwalten.

Managed Detection and Response (MDR): Lagern Sie Ihren Cyberschutz an unsere erfahrenen Experten aus. Die Threat Hunter von Kaspersky monitoren Telemetriedaten Ihrer IT-Systeme und decken Verdächtiges sofort auf. Für diesen 24/7-Service sind unsere internationalen Spezialisten in Security Operations Centern (SOC) weltweit aktiv.

Awareness Training: Kaspersky hat ein effektives Gesamtkonzept zum Aufbau von Cybersicherheits-Know-how im Unternehmen entwickelt. Die Bandbreite reicht von allgemeinen Trainings, die Ihr Team sensibilisieren und motivieren, über Fachschulungen für Help-Desk-Mitarbeiter bis zum Online-Training für Manager. Unsere interaktive Trainingsplattform Kaspersky Automated Security Awareness Platform (ASAP) bietet praxisnahe Security-Awareness-Schulungen, die sich leicht in den Arbeitsalltag integrieren lassen. Die Teilnehmer können die Lernmodule flexibel online durcharbeiten.

Threat Intelligence (TI): Mit der branchenführenden Threat Intelligence (TI) von Kaspersky gewinnen Unternehmen einen unverzichtbaren 360-Grad-Blick auf die Bedrohungslandschaft. Sie erhalten damit Zugriff auf die umfassende Gefährdungsdatenbank und das Expertenwissen von Kaspersky im IT- und OT-Umfeld. So können sie drohende Angriffe frühzeitig erkennen, Sicherheitsmaßnahmen verstärken und ihre Systeme gezielt härten.

Incident Response (IR): Bei einem Sicherheitsvorfall haben gut vorbereitete Unternehmen den Vorteil, dass sie schneller und effizienter reagieren können. Kaspersky bietet eine Reihe von Incident Response Services an, um Organisationen bei der Vorbereitung auf einen Cybervorfall zu unterstützen. So ist Kaspersky Tabletop Exercise (TTX) eine angeleitete Übung, mit der Sie Ihre Prozesse und Pläne zur Vorfallreaktion überprüfen. Dadurch identifizieren Sie Lücken in Ihrem Notfallplan, klären die Rollen und Verantwortlichkeiten der Teams und verbessern die Koordination zwischen den Abteilungen.

Industrial Cybersecurity: Kaspersky Industrial Cybersecurity (KICS) ist eine bewährte und zertifizierte Industrielösung, die den spezifischen Cybersicherheitsanforderungen von Industrieunternehmen und Betreibern kritischer Infrastrukturen entspricht. KICS schützt bereits mehr als 1.000 High-End-Industriekunden weltweit.

External Attack Surface Management (EASM): Mit Kaspersky Digital Footprint Monitoring können Unternehmen ihre gesamte digitale Präsenz kontinuierlich überwachen und potenzielle Bedrohungen aus dem öffentlichen Internet, Deep Web und Dark Web frühzeitig erkennen. Dadurch erhalten sie einen vollständigen Überblick über ihre Angriffsfläche sowie mögliche externe Exposures und können Risiken gezielt abwehren, bevor diese zu finanziellen Verlusten oder Rufschäden führen.

Log Collector/SIEM (Security Information and Event Management): Diese Lösungen unterstützen Unternehmen dabei, Anforderungen im Zusammenhang mit der DSGVO, NIS 2, PCI DSS, internen Audit- und Vorfallreaktionsprozessen sowie unternehmensinternen Richtlinien zur Protokollaufbewahrung zu erfüllen. Sie zentralisieren und sichern Protokolle über verteilte IT-Umgebungen hinweg und tragen so dazu bei, die Integrität und Verfügbarkeit der erfassten Protokolldaten zu gewährleisten. Dadurch können Unternehmen bei einem Audit oder Incident compliant handeln und Nachweispflichten erfüllen.

Kaspersky kennt die Anforderungen verschiedener Branchen und Unternehmensgrößen genau und **schützt weltweit über 200.000 Unternehmen** gegen Cyberbedrohungen.

Suchen Sie einen einfach zu verwaltenden Baukasten für mehr Cybersicherheit und Compliance? **Zusammen finden wir die passgenaue Lösung für Ihr Unternehmen.**

Sprechen Sie uns an!
kaspersky.de/go/nis-2

Cyber Threat News: de.securelist.com
IT Security News: kaspersky.de/blog/b2b
IT-Sicherheit für SMB: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise-security

kaspersky.de