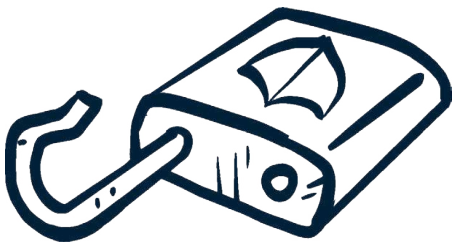
Cyberangriffe: Manager haften selbst



Gastbeitrag. In sechs Monaten treten strengere Regeln zum Schutz vor Attacken aus dem Web in Kraft. Fehlerhafte Umsetzung macht nicht nur Unternehmen strafbar; auch Leitungsorgane werden zahlungspflichtig.

VON MARTIN KOLLAR
UND DAVID BLUM

Wien. Es sind nicht gerade sprechende Abkürzungen: Dora, Nis-2, CER. Dahinter steht ein umfassendes Paket europäischer Vorgaben zur Cybersicherheit und Resilienz in Unternehmen. Die Maßnahmen sollen die Widerstandsfähigkeit gegenüber Attacken stärken. Ab Oktober 2024 gelten für Tausende Unternehmen in Österreich verpflichtend strenge Vorgaben zur Cybersicherheit nach dem neuen Nis-Gesetz. Bei vielen Unternehmen fehlt aber noch das Bewusstsein für den dringenden Handlungsbedarf. Denn bei einer mangelhaften Umsetzung drohen nicht nur dem Unternehmen Geldstrafen in Millionenhöhe. Auch das Management und der Aufsichtsrat können nach dem Nis-Gesetz persönlich für entstandene Schäden haften.

In der Finanzbranche wurden schon im Jahr 2023 mit der EU-Verordnung Dora (Digital Operational Resilience Act) strenge Vorgaben für die Cybersicherheit implementiert, die bis Anfang 2025 umzusetzen sind. Parallel werden durch die CER-Richtlinie (Critical Entities Resilience Directive) für die kritische Infrastruktur strenge Vorgaben für die physische Sicherheit eingeführt. Dazu müssen die EU-Mitgliedstaaten Unternehmen identifizieren, die als kritische Infrastruktur gelten, und bis 2026 eine nationale Risikobewertung durchführen.

Mehr Unternehmen erfasst

Während Dora nur für die Finanzbranche gilt und die CER-Richtlinie nur einzelne Einrichtungen der kritischen Infrastruktur erfasst, gelten die Cybersecurity-Vorgaben der Nis-2-Richtlinie (Network and Information Security Directive) für eine Vielzahl von Unternehmen. Die Richtlinie ist bis 18. Oktober 2024 durch die Mitgliedstaaten umzusetzen. In Österreich wurde vor Kurzem der Ministerialentwurf zum neuen Nis-Gesetz veröffentlicht. Den betroffenen Unternehmen bleiben zur Umsetzung der neuen Vorgaben nur noch wenige Monate Zeit.

Der Anwendungsbereich des neuen Nis-Gesetzes wird durch Nis-2 erheblich erweitert. Während das aktuelle Gesetz in ganz Österreich nur rund 100 Unternehmen als „Betreiber wesentlicher Dienste" erfasst, müssen nach der geplanten neuen Fassung rund 6500 Unternehmen die umfangreichen Cybersecurity-Vorgaben umsetzen. Konkret unterscheidet Nis-2 zunächst zwischen „Sektoren mit hoher Kritikalität" und „Sonstigen kritischen Sektoren".

In den hochkritischen Bereich fallen die Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Verwaltung von IKT-Diensten, öffentliche Verwaltung und Weltraum. Sonstige kritische Sektoren sind Post, Abfallbewirtschaftung, Chemie, Lebensmittel, verarbeitendes Gewerbe, digitale Dienste und Forschung. Damit deckt Nis-2 weite Teile der gesamten Wirtschaft ab.

Komplexe Berechnung

Das neue Nis-Gesetz gilt für Unternehmen, die mittelgroß oder größer sind, das heißt bereits ab mehr als 50 Beschäftigten und über zehn Millionen Euro Umsatz. Schon die Abgrenzung, ob ein Unternehmen als zumindest mittelgroß gilt, kann sehr komplex sein. Denn dabei müssen auch die Mitarbeiterzahlen, der Umsatz und die Jahresbilanzsumme vor- oder nachgeschalteter Partnerunternehmen sowie verbundener Unternehmen berücksichtigt werden.

Als Partnerunternehmen gelten Unternehmen, die 25 Prozent oder mehr des Kapitals oder der Stimmrechte eines anderen Unternehmens halten. Verbundene Unternehmen üben - etwa über die Mehrheit der Stimmrechte - Kontrolle über ein anderes Unternehmen aus. Die Anrechnung der Kennzahlen erfolgt bei Partnerunternehmen proportional zur Höhe der Beteiligung, bei verbundenen Unternehmen zu 100 Prozent. Durch diese Zusammenrechnung können auch kleinste Unternehmen von Nis-2 betroffen sein.

Ob Unternehmen in den Anwendungsbereich von Nis-2 fallen oder nicht, müssen sie (mit wenigen Ausnahmen) selbst prüfen und sich bei der zuständigen Behörde registrieren. Bei vielen Unternehmen besteht aber noch kein Bewusstsein dafür, dass sie Nis-2 unterliegen und ihnen damit nur noch wenige Monate zur Umsetzung der neuen Cybersecurity-Vorgaben bleiben. Dazu gehören insbesondere die Einrichtung eines umfassenden Risikomanagements, der Einsatz geeigneter Verschlüsselungen, Zugangskontrollen und Multifaktor-Authentifizierungen sowie strenge Melde- und Berichtspflichten an die Behörde. In der Praxis besonders herausfordernd ist die Verpflichtung der Unternehmen, nicht nur ihre eigene Cybersicherheit zu prüfen, sondern diese auch in der Lieferkette sicherzustellen. Dadurch betrifft Nis-2 indirekt auch alle Dienstleister und Lieferanten dieser Unternehmen.

Wie wichtig es ist, mit der Umsetzung von Nis-2 zu starten, macht ein Blick auf die Straf- und Haftungsbestimmungen deutlich. Der vorliegende Gesetzesentwurf sieht einen sehr umfassenden Katalog an Straftatbeständen vor, die von der Verletzung rein administrativer Meldepflichten bis hin zu gravierenden Verstößen reichen. Die Mindeststrafdrohungen betragen sieben Millionen Euro für „wichtige" und zehn Millionen Euro für „wesentliche" Unternehmen.

Für das Management und den Aufsichtsrat äußerst heikel ist eine Haftungsfalle, die sich unmittelbar aus Nis-2 ergibt. Denn Nis-2 sieht eine Verpflichtung zur Einführung eines Risikomanagements für Cybersicherheit vor. Das Risikomanagement muss dem Stand der Technik entsprechen, auf einem gefahrenübergreifenden Ansatz beruhen und auch die Überprüfung der Lieferketten einschließen. Entspricht das Risikomanagement nicht den Vorgaben der Nis-2, haften die Leitungsorgane persönlich für den entstandenen Schaden. Sie können daher persönlich zur Haftung herangezogen werden, wenn dem Unternehmen durch eine Cyberattacke ein Schaden entsteht. Derartige Schäden können sich etwa aus einer Betriebsunterbrechung, den Kosten der Datenwiederherstellung oder der Zahlung von Lösegeldern an Hacker ergeben. Ob Unternehmen von ihren Leitungsorganen auch Schadenersatz verlangen können, wenn die Behörde Verwaltungsstrafen - potenziell in Millionenhöhe - gegen sie verhängt, ist dagegen umstritten.

Versicherungen zu empfehlen

Bemerkenswert ist auch der Begriff der „Leitungsorgane" im Ministerialentwurf, der nach den Erläuterungen die „tatsächliche Leitungs- und Geschäftsführungsebene" erfassen soll. Dies umfasst jedenfalls das Management und den Aufsichtsrat des Unternehmens. Denkbar wäre aufgrund der Weisungskette aber auch eine persönliche Haftung der Konzernführung für Verstöße in verbundenen Unternehmen. Um sich vor einer persönlichen Haftung zu schützen, müssen Leitungsorgane daher rechtzeitig die Einrichtung eines entsprechenden Risikomanagements sicherstellen. Empfehlenswert ist weiters die Absicherung des Unternehmens durch eine Cyber-Versicherung und der Leitungsorgane durch eine D&O-Versicherung.

Weil die neuen Nis-2-Vorgaben schon ab 18. Oktober 2024 gelten, müssen Unternehmen so bald wie möglich prüfen, ob sie betroffen sind. Ist das der Fall, sollten sie eine Risikobeurteilung durchführen, um potenzielle Sicherheitslücken zu identifizieren, und adäquate technische und organisatorische Sicherheitsmaßnahmen implementieren, um Cybersicherheitsrisken und die zukünftig notwendigen Meldepflichten effektiv zu managen. Ein weiterer wichtiger Schritt ist die Entwicklung eines ganzheitlichen Resilienzplans. Für Unternehmen, die sich noch nicht mit den neuen Vorgaben auseinandergesetzt haben, besteht dringender Handlungsbedarf. Die Zeit drängt.

Martin Kollar ist Rechtsanwalt und Gründungspartner bei der Wirtschaftskanzlei Akela.
David Blum arbeitet bei Accenture Österreich. Zuvor war er stellvertretender Direktor der Direktion Staatsschutz und Nachrichtendienst (DSN).

LEGAL § PEOPLE

Branchen-News aus der Welt des Rechts

Events der Woche

Das Institut für Zivil- und Zivilverfahrensrecht der WU Wien lud gemeinsam mit dem Österreichischen Rechtsanwaltskammertag (ÖRAK) und der Anwaltsakademie zum zweiten Zivilrechtstag der Österreichischen Rechtsanwältinnen und Rechtsanwälte. Mehr als 400 Standesangehörige aus ganz Österreich nutzten die Möglichkeit, sich über neueste Entwicklungen in den Bereichen Zivil- und Zivilverfahrensrecht sowie im Unternehmensrecht zu informieren. Die Veranstaltung wird auch im nächsten Jahr wieder stattfinden. Save the Date: 7. April 2025.

Berthold Hofbauer, Heid & Partner, und Gregor Biley, NHP. [beigestellt]

Die etablierte Webinarreihe „VERUM aktuell" bot seinen 300 Teilnehmern und Teilnehmerinnen spannende Einblicke in die Themen Lieferketten und Greenwashing, über die die Experten **Gregor Biley,** Rechtsanwaltsanwärter bei NHP, und **Berthold Hofbauer,** Heid & Partner, informierten. Veranstaltet wurde das Webinar von den beiden Rechtsanwaltskanzleien Heid & Partner sowie Niederhuber & Partner.

CHG Managing-Partner Günther Gast und Dietmar Czernich. [DieFotografen]

Mitte April hat CHG Rechtsanwälte, die größte Wirtschaftskanzlei Westösterreichs, ihr neues Meeting Center im Zentrum von Innsbruck offiziell eröffnet und bei dieser Gelegenheit auch gleich das 25-jährige Bestehen der Kanzlei gefeiert. CHG Rechtsanwälte wurde im Jahr 1999 von **Dietmar Czernich** gegründet und hat mittlerweile auch Standorte in Wien, Vaduz (Liechtenstein), Bozen (Italien) und St. Johann/Kitzbühel. Unter den zahlreichen Gästen und Gratulanten waren unter anderem WKT-Präsidentin **Barbara Thaler** und Univ.-Prof. **Arno Kahl.**

Sibylle Novak, Partnerin bei CMS Österreich. [CMS]

Aus der Feder von KWR-Partner **Thomas Haberer** stammt eine Neuauflage des von **Heinz Krejci** begründeten Werkes zum Gesellschaftsrecht Allgemeiner Teil. In der beim Manz Verlag erschienenen Publikation findet man eine tiefgehende Darstellung der Grundstrukturen des Gesellschaftsrechts, ergänzt um einen praxisorientierten Rechtsformenvergleich.

Deal der Woche

Der international operierende Energietechnikkonzern Siemens Energy hat seine Sparte für Hochspannungskomponenten, Trench Electric, an den Finanzinvestor Triton verkauft. Siemens Energy setzte beim Verkauf auf die steuerrechtliche Expertise von CMS Österreich. Neben Partnerin **Sibylle Novak** waren die Rechtsanwälte **Thomas Aspalter** und **Bernhard Oreschnik** an der Transaktion beteiligt. Das internationale CMS-Team unter der Federführung von Partner **Jörg Schrade** (CMS Deutschland) umfasste mehrere Jurisdiktionen.

LEGAL & PEOPLE

ist eine Verlagsserie der „Die Presse" Verlags-Gesellschaft m.b.H. & Co KG
Koordination: René Gruber
E-Mail: rene.gruber@diepresse.com
Tel.: +43/(0)1/514 14 263