SBS | LEGAL
Rechtsanwälte

Cyberangriffe:
Eine unterschätzte Gefahr mit verheerenden Folgen

SBS | LEGAL
Rechtsanwälte

Cyberangriffe: Eine unterschätzte Gefahr mit verheerenden Folgen

Die Digitalisierung ist eine der größten Chancen der letzten Jahrzehnte – aber auch eine der größten Risiken. Cyberangriffe nehmen in Frequenz und Intensität zu und stellen eine existenzielle Bedrohung für Unternehmen dar.

Ob Datenverluste, massive Schadensersatzansprüche nach Betriebsstillstand oder Reputationsschäden: Die Frage ist nicht mehr, ob Sie angegriffen werden, sondern wann. Sind Sie darauf vorbereitet?

Warum **jetzt** zu Handeln entscheidend ist

Mit der Einführung der DORA- und NIS-2-Regulierungen und vor allem durch die Fortentwicklung der Rechtssprechung zur DSGVO ab 2025 wird der Druck auf Unternehmen weiter steigen. Die EU schreibt strenge Anforderungen an Cybersicherheit vor, die von Ihnen als Geschäftsführung konsequent umgesetzt werden müssen.

DSGVO

Warum die DSGVO im Bereich Cybersicherheit zu einem sehr scharfen Schwert geworden ist

Die bereits seit 2018 in Kraft befindliche DSGVO gewinnt drastisch mehr an Schärfe. Deutsche und EU-Datenschutzbehörden haben in 2024 eine Reihe von Bußgeldern in fünf- und sechsstelliger Höhe bei Datenschutzverletzungen verhängt. Neueste Urteile des EuGH und BGH aus Oktober 2024 haben klargestellt, dass Unternehmen für Datenschutzverletzungen auch ohne Nachweis eines erheblichen Schadens haften werden und dieser Schaden schnell 100.000 € und mehr betragen kann.

Ignoranz ist also keine Option mehr, **DENN** die DSGVO gilt für **ALLE** Unternehmen (und nach einer weiteren Entscheidung des EUGH aus 2018 können auch deren CEO haften), die Kundendaten nutzen – dies kann der Friseur oder Kfz-Meister von nebenan, die Online-Apotheke oder ein anderer Online-Shop sein, ebenso wie Ärzte, Zahnärzte, Physiotherapeuten, Steuerberater, Makler, Handelsvertreter oder Direktvertriebe sein.

Diese Entscheidungen der Behörden und Gerichte aus 2024 erhöhen somit den Druck auf Unternehmen, ihre IT-Sicherheitsmaßnahmen umfassend zu dokumentieren und regelmäßig zu aktualisieren und viel wichtiger, Ihre IT-Infrastruktur von **INNEN** (wie auch von außen) zu schützen. Die persönliche Haftung der Geschäftsführung rückt damit noch stärker in den Fokus.

BITTE MERKEN SIE SICH:

Ein Versäumnis der Sicherung der IT-Infrastruktur und der Kundendaten kann nicht nur Ihr Unternehmen in den Ruin treiben, sondern auch Sie als CEO persönlich teuer zu stehen kommen.

Wir sind überzeugt, dass wir Sie und Ihr Unternehmen rechtssicher aufstellen können.

Art. 32 DSGVO
– was Sie wissen müssen

Artikel 32 DSGVO verpflichtet alle Unternehmen, die Kundendaten nutzen, zur Umsetzung technischer und organisatorischer Maßnahmen, um ein angemessenes Schutzniveau zu gewährleisten. Dabei wird insbesondere gefordert:

- der Schutz der IT-Infrastruktur und zwar von **INNEN** und außen
- Verschlüsselung sensibler Daten
- Regelmäßige Prüfungen der IT-Sicherheitsmaßnahmen
- Schnelle Reaktion auf Sicherheitsvorfälle

Die Praxis zeigt jedoch: Viele Unternehmen erfüllen diese Anforderungen gar nicht oder nur unzureichend. Ein Verstoß kann nicht nur zu den bereits benannten hohen Bußgeldern und massiven Schadensersatzforderungen führen.
Vielmehr droht ein immenser Imageverlust bei Bekanntwerden eines erfolgreichen Angriffs auf die IT-Infrastruktur. Es drohen sehr hohe Kosten durch einen ggf. erforderlichen Austausch der IT-Infrastruktur und der erforderlichen Kommunikation mit Kunden und Behörden unter Hinzuziehung von Fachanwälten.

DORA & NIS-2
– was Sie wissen müssen

DORA: Der Digital Operational Resilience Act - Die DORA-Verordnung zielt darauf ab, die digitale Resilienz der Finanzbranche zu stärken.

Sie fordert:
- den Schutz der IT-Infrastruktur und zwar von **INNEN** und außen
- Regelmäßige Prüfungen und Tests der IT-Sicherheitsinfrastruktur
- Strikte Sicherheitsmaßnahmen und proaktive Schwachstellenanalysen
- Umfassende Meldepflichten bei Sicherheitsvorfällen

FÜR WEN GELTEN DORA UND NIS-2:
Die DORA gilt für die Unternehmen aus dem Finanzsektor, wie z.B.: Zahlungsinstitute, Versicherungen, Wertpapierunternehmen, ebenso wie für Anbieter von Krypto-Dienstleistungen (MiCA), Assekuradeure, Finanzdienstleister und Versicherungsmakler/-vermittler (ab einer gewissen Größe).

Die NIS-2-Richtlinie betrifft nicht nur große, sondern zunehmend auch mittlere Unternehmen aus Branchen wie Energie, Transport, Gesundheit, digitale Infrastruktur und öffentliche Verwaltung.

Die Konsequenzen:
Unternehmen müssen erheblich in ihre IT-Sicherheitsinfrastruktur investieren und sind verpflichtet, Vorfälle öffentlich zu machen – ein Reputationsrisiko, das Sie ernst nehmen sollten.

SBS | LEGAL
Rechtsanwälte

Das Ziel ist klar:

Unternehmen müssen widerstandsfähiger gegenüber Cyberangriffen werden und das Vertrauen in digitale Dienste und den Schutz der Kundendaten stärken.

Die NIS-2-Richtlinie betrifft nicht nur große, sondern zunehmend auch mittlere Unternehmen aus Branchen wie Energie, Transport, Gesundheit, digitale Infrastruktur und öffentliche Verwaltung.

Sie verlangt:

- den Schutz der IT-Infrastruktur und zwar von **INNEN** und außen
- Einheitliche Sicherheitsstandards für kritische Infrastrukturen
- Sicherheitsmaßnahmen, wie Penetrationstests und Krisenmanagement
- Schnelle Berichterstattung bei Vorfällen – innerhalb von 72 Stunden.

DIE KONSEQUENZEN:

Virenscanner und Firewalls sind mittlerweile in den allermeisten Unternehmen vorhanden, jedoch fehlt es bei den Unternehmen fast immer an dem technischen Schutz der Infrastruktur von **INNEN**.

Zwingend notwendig ist es daher, dass alle Unternehmen umfassend in ihre IT-Sicherheitsinfrastruktur investieren, um den gesetzlichen Anforderungen gerecht zu werden, denn 99% und mehr der Cyberangriffe entstehen von **INNEN** z.B. durch das Öffnen von toxischen E-Mails oder Anhängen durch Mitarbeiter.

Das Geschäft
und die Gefahr der Cyberindustrie

Cyberkriminelle werden immer professioneller.

Ihre Ziele:

- Finanzieller Gewinn: Ransomware verschlüsselt Ihre Systeme. Unternehmen zahlen häufig Millionenbeträge, um wieder handlungsfähig zu sein.
- Datendiebstahl: Kundendaten, Geschäftsgeheimnisse und geistiges Eigentum sind eine lukrative Beute.
- Reputationsschäden: Ein Cybervorfall kann Vertrauen zerstören, das über Jahre aufgebaut wurde.

Die Folgekosten sind enorm und umfassen insbesondere:

- Reparatur und Wiederherstellung der IT-Infrastruktur
- Forensische Untersuchungen
- Drastische Bußgelder und Schadensersatzansprüche
- Kostspielige Rechtsberatung und Krisenkommunikation

Ein erfolgreicher Angriff kann Ihr Unternehmen in den Ruin treiben.

Ihre Verantwortung als Geschäftsführung

Mit DORA, NIS-2 und den verschärften DSGVO-Anforderungen stehen Sie persönlich in der Pflicht:

1. Haftungsrisiko: Sie haften, wenn IT-Sicherheitsmaßnahmen als unzureichend gelten und die Anforderungen der EUGH Rechtssprechung erfüllt sind.
2. Meldepflichten: Sicherheitsvorfälle müssen schnell und umfassend dokumentiert und gemeldet werden.
3. Investitionen: Moderne IT-Sicherheitslösungen sind kein optionaler Luxus.

Vielmehr bilden sie die unverzichtbare Grundlage für die Erfüllung der geschäftsmäßigen Sorgfaltspflicht einer jeden Geschäftsführung.

Die Kernbotschaft:

Schützen Sie nicht nur Ihr Unternehmen, sondern auch sich selbst als verantwortlich handelnde Person.

SBS | LEGAL
Rechtsanwälte

SBS Legal

Ihr Partner für Cybersicherheit und Compliance

Unser Team aus Fachanwält:innen und spezialisierten Rechtsanwält:innen bietet Ihnen maßgeschneiderte Lösungen.

- Analyse Ihrer Betroffenheit: Wir prüfen, ob Ihr Unternehmen unter die Regeln der DSGVO, DORA und/oder NIS-2 fällt.
- Erstellung von Sicherheitskonzepten: Lösungsorientierte Umsetzung und Begleitung zur rechtlichen Absicherung Ihrer IT-Infrastruktur und maßgeschneiderte Strategien zur Minimierung Ihrer Risiken.
- Haftungsminimierung: Wir schützen Sie vor rechtlichen Konsequenzen und sorgen für die Einhaltung der gesetzlichen Vorgaben.
- Darüber hinaus arbeiten wir mit spezialisierten Partnern zusammen, um Ihnen ganzheitliche Unterstützung zu bieten – von der IT-Sicherheit bis zur Krisenkommunikation.

Jetzt handeln, bevor es zu spät ist

Die Herausforderungen durch DSGVO, DORA und NIS-2 sind zwar exorbitant – aber auch im finanziell angemessen Rahmen lösbar.

Nutzen Sie unsere Expertise, um sich rechtlich und über unsere Partner auch technisch abzusichern.

Kontaktieren Sie uns:

- E-Mail: dora@sbs-legal.de

- Telefon: +49 40-734 40 860

Schützen Sie Ihre Zukunft.

Der nächste Angriff kommt bestimmt – seien Sie vorbereitet.

Herausgeber

SBS | LEGAL
Rechtsanwälte

Version: DE/AT-DE-2501