

Pflichten und Haftung der Geschäftsführung im Unternehmen

Cybersecurity & Datenschutz

Ing. Mag. Jürgen Hutsteiner, CIPP/E



RA Mag. Toni Brnada





- Ablauf

Zwei Teile

01 Ausgangslage

Warum sich die Lage 2026 verändert hat

02 Betroffenheit

Wen rechtliche Sicherheitsanforderungen treffen

03 Anforderungen

Die Pflichten im Klartext

04 Best Practice

Was im Unternehmen wirklich hilft

05 Haftung

RA Brnada: Wer haftet wofür

06 Absicherung

RA Brnada: Wie man sich schützt



01

Ausgangslage

Warum das Thema Cybersecurity jetzt so relevant ist

Vier Entwicklungen, die zusammenfallen

● 01 Ausgangslage

Vier Entwicklungen, die zusammenfallen



Gesetze: Das NISG 2026 gilt ab 1. Oktober 2026 — Cyber Resilience Act teilweise ab 11. September 2026



Lieferkette: Auftraggeber verlangen Sicherheitsnachweise vertraglich, auch von nicht erfassten Betrieben



Cyberangriffe: Die Anzahl an Cyberangriffen steigt. Hacken wird durch KI erleichtert.



Versicherung: Cyberpolizzen prüfen Obliegenheiten wie MFA und Backup vor der Deckung



01 Ausgangslage

Aktuelle Cyberangriffe

Gesamtdelikte bleiben hoch — doch Angriffe auf IT-Systeme und Unternehmen steigen weiter.

63.459

Cybercrime-Anzeigen 2025 (AT)

+1,8 % ggü. 2024 · weiter auf hohem Niveau

+8,6 %

Cybercrime im engeren Sinn

2025: 21.988 Angriffe auf IT-Systeme

2.243

Angriffe je Organisation/Woche

Juni 2026 · +37 % ggü. Vorjahr · Check Point

Was sich verändert

- Betrug –2,4 %, Systemangriffe +8,6 %
- Schaden Investitionsbetrug: ~120 Mio. € (2025)
- KI & Deepfakes verstärken die Angriffe

EU-Einordnung · ENISA 2025

- DDoS dominiert: 77 % der Vorfälle
- Ransomware bleibt am folgeschwersten
- KI & Info-Stealer verstärken Angriffe

Quellen: BK Cybercrime Report 2025 · Check Point Research, Monthly Report Juni 2026 · ENISA Threat Landscape 2025.



● 01 Ausgangslage

Die Stufen des NISG 2026

1. Oktober 2026

In Kraft

1

Risikomanagement, Meldewege
und Verantwortlichkeiten müssen
stehen

31. Dezember 2026

Registrierung

2

Meldung beim Bundesamt für
Cybersicherheit, drei Monate ab
Inkrafttreten

30. September 2027

Selbstdeklaration

3

Beschreibung der Maßnahmen
samt Ergebnis der Risikoanalyse

danach

Prüfbericht

4

Nachweis der Wirksamkeit durch
eine unabhängige Stelle



02

Betroffenheit

Gilt das überhaupt für unseren Betrieb?

Sektor · Schwellenwerte · Lieferkette

Drei Möglichkeiten der Betroffenheit



01

Direkt erfasst

Sektor nach Anlage 1 oder 2 und Schwellenwert erreicht: ab 50 Beschäftigten oder 10 Mio. Euro Umsatz.



02

Über die Lieferkette

Erfasste Kunden müssen ihre Lieferanten steuern. Die Anforderung kommt über den Vertrag, nicht über das Gesetz.



03

Über die DSGVO

Art. 32 DSGVO gilt unabhängig von Größe und Sektor. Sicherheit der Verarbeitung ist keine NIS-Frage.

Zwei Regelwerke, gemeinsame Anforderungen



DSGVO

SEIT 2018, KEINE SCHWELLENWERTE

- Schutzgut: personenbezogene Daten
- Kernpflicht: Art. 32 — angemessene technische und organisatorische Maßnahmen
- Aufsicht: Datenschutzbehörde, meist anlassbezogen
- Rahmen: bis 20 Mio. Euro oder 4 Prozent



NISG 2026

AB 1. OKTOBER 2026, SEKTOREN UND SCHWELLEN

- Schutzgut: Verfügbarkeit und Integrität der Systeme
- Kernpflicht: § 32 — Risikomanagement mit zehn Maßnahmenfeldern
- Aufsicht: Bundesamt für Cybersicherheit
- Rahmen: bis 10 Mio. Euro oder 2 Prozent

Die zugrunde liegenden technischen und organisatorischen Maßnahmen überschneiden sich im Kern weitgehend.



03

Anforderungen

Was konkret zu tun ist

Die zehn Maßnahmenfelder und die Pflichten der
DSGVO

- 03 Anforderungen

Die zehn Maßnahmenfelder (1 bis 5)

Nr.	Maßnahmenfeld nach § 32 NISG 2026	Was das im Unternehmen heißt
1	Risikoanalyse und Sicherheitspolitik	Ein Risikoregister, jährlich aktualisiert, von der Geschäftsführung beschlossen
2	Bewältigung von Sicherheitsvorfällen	Notfallplan mit Meldekette, Rollen und Erreichbarkeiten — einmal geübt
3	Betriebskontinuität und Backup	Backup nach der 3-2-1-Regel, dokumentierter Restore-Test
4	Sicherheit der Lieferkette	Lieferantenliste mit Kritikalität, Sicherheitsklauseln in den Verträgen
5	Sicherheit in Beschaffung und Entwicklung	Patchmanagement mit Fristen, Umgang mit gemeldeten Schwachstellen

- 03 Anforderungen

Die zehn Maßnahmenfelder (6 bis 10)

Nr.	Maßnahmenfeld nach § 32 NISG 2026	Was das im Unternehmen heißt
6	Bewertung der Wirksamkeit	Kennzahlen, eine interne Prüfung, dokumentierte Nachschärfung
7	Cyberhygiene und Schulung	Awareness einmal jährlich mit Teilnehmerliste, Phishing-Simulation
8	Kryptografie	Verschlüsselung von Notebooks und Datenträgern, eine Regel dazu
9	Personalsicherheit und Zugriffskontrolle	Rechtekonzept, geregeltes On- und Offboarding, Umgang mit Adminrechten
10	Multi-Faktor-Authentifizierung	MFA für Fernzugriff, E-Mail und alle administrativen Konten

- 03 Anforderungen

Von der Pflicht zur konkreten Maßnahme

1

NIS-2 Art. 21 / § 32 NISG — grundlegende Anforderungen

Prinzipienbasiert: Sie definiert das Was — Risikomanagement, Lieferkette, Kryptografie, Cyberhygiene — nicht das Wie.



2

DVO (EU) 2024/2690, Anhang — technische Anforderungen

Unmittelbar anwendbar, ohne nationale Umsetzung; legt auch fest, wann ein Vorfall „erheblich“ ist. Gilt direkt für die Digital-Sektoren.



3

ENISA-Leitfaden 6/2025 — konkrete Umsetzung

Kontrollbeispiele und Nachweise mit Zuordnung zu ISO 27001. Nicht bindend, aber maßgeblich.

Für alle übrigen NISG-Betriebe konkretisiert § 32 NISG die Maßnahmen — **DVO-Anhang und ENISA-Leitfaden dienen als Maßstab.**

- 03 Anforderungen

Was die DSGVO davon unabhängig verlangt



Verarbeitungsverzeichnis

Art. 30



Angemessene Sicherheit

Art. 32 — Maßnahmen und deren Begründung



Meldung binnen 72 Stunden

Art. 33 — an die Datenschutzbehörde



Auftragsverarbeiter

Art. 28 — AVV samt Kontrolle des Dienstleisters



Betroffenenrechte

Art. 15 ff. — Prozess und Frist von einem Monat



Löschkonzept

Art. 5 — Fristen je Datenkategorie, umgesetzt



- 03 Anforderungen

Vier Fristen im Ernstfall



24 Stunden: Frühwarnung an das Bundesamt für Cybersicherheit (§ 34 NISG 2026)



72 Stunden: Vorfallsmeldung nach NISG, parallel Meldung an die Datenschutzbehörde (Art. 33 DSGVO)



1 Monat: Abschlussbericht zum Vorfall nach NISG, ebenso Frist für Auskunft an Betroffene (Art. 15 DSGVO)



Bei hohem Risiko unverzüglich: Information der betroffenen Personen (Art. 34 DSGVO)



04

Best Practice

Was im Unternehmen wirklich funktioniert

Sechs Maßnahmen und der Unterschied zwischen
Papier und Nachweis



● 04 Best Practice

Sechs Maßnahmen mit dem besten Verhältnis



MFA überall

Fernzugriff, E-Mail, Adminkonten.
Verhindert den häufigsten
Einstiegsweg.



Backup mit Restore-Test

Offline-Kopie und ein
protokollierter
Wiederherstellungstest pro Jahr.



Patchen mit Frist

Kritische Lücken in Tagen, nicht in
Quartalen. Frist schriftlich
festlegen.



Awareness und Phishing

Eine Schulung jährlich, eine
Simulation. Mit Teilnehmerliste.



Rechte aufräumen

Keine Dauer-Adminrechte,
geregeltes Offboarding am
Austrittstag.



Notfallplan üben

Eine Seite, ausgedruckt, mit
Meldekette. Kommunikation
regeln. Einmal im Jahr
durchgespielt.

Was im Prüf- und Haftungsfall zählt

✓ Zählt

- Freigabe durch Geschäftsführung mit Datum
- Protokoll des Restore-Tests
- Teilnehmerliste der Schulung
- Benannte Verantwortliche mit Erreichbarkeit
- Nachweis, dass Maßnahmen geprüft wurden

✗ Zählt nicht

- Richtlinie ohne Freigabe und ohne Umsetzung
- Gekauftes Werkzeug ohne Prozess dahinter
- Backup, das nie zurückgespielt wurde
- Zuständigkeit „die IT macht das“
- Zertifikat des Dienstleisters als eigener Nachweis



Nicht dokumentiert heißt nicht getan.

Maßnahmen erfordern nicht nur **Wirksamkeit**,
sondern auch **Nachweisbarkeit**.



05

Haftung

Wer haftet — und wofür

Teil 2 · RA Mag. Toni Brnada

summereder
pichler
wächter
stehrer



grander
brnada
harringer
pröll

rechtsanwälte



- Teil 2 · RA Mag. Toni Brnada

Was in den nächsten 25 Minuten kommt

- 01 Haftungsarchitektur**
Gesellschaft, Organ, Mitarbeiter — wer steht wo
- 02 Verwaltungsstrafen**
Wen die Behörde adressiert und in welcher Höhe
- 03 Rechtsprechung**
Was österreichische Gerichte bisher entschieden haben
- 04 Der Regress**
Der Weg vom Unternehmensschaden zum Privatvermögen
- 05 Absicherung**
Organisation, Dokumentation, Versicherung

Innenhaftung und Außenhaftung



Innenhaftung

ORGAN GEGENÜBER DER GESELLSCHAFT

- § 25 GmbHG: Sorgfalt eines ordentlichen Geschäftsmannes
- § 22 Abs. 1 GmbHG: Pflicht zum internen Kontrollsystem
- Anknüpfung: Organisations-, Auswahl- und Überwachungsfehler
- Kein Dienstnehmerhaftungsprivileg für Geschäftsführer



Außenhaftung

GESELLSCHAFT GEGENÜBER DRITTEN

- Art. 82 DSGVO: Schadenersatz an betroffene Personen
- Vertragliche Haftung gegenüber Kunden bei Ausfall
- Verwaltungsstrafen der Behörde treffen die Einrichtung
- Rückgriff auf das Organ erfolgt im zweiten Schritt

Der praktisch gefährliche Weg für die Geschäftsführung führt nicht über die Behörde, sondern über den Regress der eigenen Gesellschaft.



- 05 Haftung

Die Strafraumen

10 Mio. €

oder 2 % Weltjahresumsatz ·
wesentliche Einrichtungen (§ 45
NISG)

7 Mio. €

oder 1,4 % Weltjahresumsatz ·
wichtige Einrichtungen (§ 45 NISG)

20 Mio. €

oder 4 % Weltjahresumsatz ·
DSGVO-Verstöße (Art. 83)

Adressat ist jeweils die Einrichtung. Gegen Leitungsorgane selbst sieht das NISG 2026 keine Verwaltungsstrafen vor — bei wesentlichen Einrichtungen ist aber ein vorübergehendes Tätigkeitsverbot möglich.

Was das NISG dem Leitungsorgan auferlegt



§ 31 Abs. 1: Die Umsetzung der Risikomanagementmaßnahmen sicherstellen und beaufsichtigen



§ 31 Abs. 2: Eigene Schulungspflicht des Organs, dazu Schulungsangebot für die Beschäftigten



Delegation: Die Ausführung ist delegierbar, die Aufsichts- und Letztverantwortung nicht



Tätigkeitsverbot: Bei wesentlichen Einrichtungen bei schweren oder wiederholten Verstößen vorgesehen

Der Leitfall: OGH 8 ObA 109/20t

Ende 2015

Der Angriff

Fake President Fraud bei einem börsennotierten Zulieferer, rund 43 Mio. Euro fließen ab.

danach

Die Klage

Die Gesellschaft klagt den früheren Vorstandsvorsitzenden auf Schadenersatz.

3. 8. 2021

Der OGH

Klage abgewiesen, keine Pflichtverletzung des Organs feststellbar.

heute

Der Maßstab

Die Methode ist notorisch. Dieselbe Verteidigung trägt nicht mehr.



Woran es hing

- Kontrollsystem war eingerichtet
- Vieraugenprinzip war überprüft
- Beklagter war nicht ressortzuständig
- Betrugstyp 2015 nicht notorisch
- Maßstab: größen- und branchengerecht

- 05 Haftung

Rechtsprechung, an der man sich orientiert

Nr.	Entscheidung	Kernaussage
1	OGH 8 ObA 109/20t (3. 8. 2021)	Kein Verschulden bei eingerichtetem Kontrollsystem und einer damals nicht notorischen Angriffsmethode
2	OGH 6 Ob 113/24x (3. 7. 2025)	Der Verstoß allein genügt nicht; der konkrete immaterielle Schaden ist nachzuweisen
3	EuGH C-300/21 (4. 5. 2023)	Keine Erheblichkeitsschwelle, aber ein Schaden ist zwingende Voraussetzung
4	EuGH C-340/21 (14. 12. 2023)	Nach einem Angriff muss das Unternehmen die Angemessenheit seiner Maßnahmen beweisen
5	EuGH C-807/21 (5. 12. 2023)	Eine Geldbuße gegen das Unternehmen setzt einen vorwerfbaren Verstoß voraus
6	EuGH C-655/23 (4. 9. 2025)	Unterlassungsanspruch und Maßstab für die Bemessung des immateriellen Schadens



Verschulden hängt an der Organisation.

Nicht daran, ob der Angriff erfolgreich war — sondern daran, was vorher vorgesehen war.



06

Absicherung

Wie man sich am besten absichert

Organisation, Dokumentation, Versicherung — in dieser
Reihenfolge



- 06 Absicherung

Drei Ebenen, in dieser Reihenfolge

01

Organisieren

Ressortverteilung schriftlich, internes Kontrollsystem, benannte Verantwortliche, klare Eskalation.

02

Dokumentieren

Entscheidungen mit Grundlage protokollieren: Beschluss der Maßnahmen, Schulungsnachweis, Restore-Test, Vorfallsakten.

03

Versichern

D&O und Cyberpolizze prüfen: Obliegenheiten, Selbstbehalt, Ausschlüsse, Nachmeldefristen.

Die Business Judgement Rule nach § 25 Abs. 1a GmbHG schützt nur die Entscheidung, deren Grundlage nachweisbar ist. Ohne Dokumentation gibt es keinen sicheren Hafen.

- 06 Absicherung

Wo die Absicherung endet

 **D&O:** Deckt typischerweise weder Vorsatz noch wissentliche Pflichtverletzung

 **Cyberpolizze:** MFA, Backup und Patchstand sind Deckungsvoraussetzung, nicht Empfehlung

 **Verwaltungsstrafen:** Sind nicht auf eine Versicherung abwälzbar

 **Entlastung:** Ein Gesellschafterbeschluss entlastet nur, was der Geschäftsführung offengelegt wurde

Sechs Fragen, die man sich stellen sollte



Betroffenheit

Ist unsere Einordnung nach dem NISG 2026 schriftlich begründet?



Wiederherstellung

Wann wurde das Backup zuletzt tatsächlich zurückgespielt?



Meldung

Wer meldet nachts binnen 24 Stunden — namentlich?



Zugänge

Wo fehlt MFA noch, und warum genau dort?



Dienstleister

Welcher Ausfall bei welchem Lieferanten stellt uns still?



Deckung

Welche Obliegenheiten verlangt unsere Polizza, und erfüllen wir sie?



- Nächste Schritte

Was dringend gemacht werden sollte

01

NIS2-Betroffenheit klären

Sektor, Schwellenwerte und Lieferkette prüfen und das Ergebnis schriftlich festhalten.

02

Lücken erheben

Ist-Stand gegen die zehn Maßnahmenfelder halten und die drei größten Lücken terminieren.

03

Beschluss fassen

Maßnahmen in der Geschäftsführungssitzung beschließen, Schulung des Organs terminieren.

Zeit für Ihre Fragen



RA Mag. Toni Brnada
Summereder Pichler Wächter Rechtsanwälte GmbH
office@spwr.at



pribizz
Consulting

Ing. Mag. iur. Jürgen Hutsteiner, CIPP/E
· pribizz consulting GmbH
· jh@pribizz.at