BlueFlag Security

INTELLECTUAL PROPERTY PROTECTION · SOLUTION BRIEF · JUNI 2026

Software-IP schützen
Vom Quellcode zur Vorstandspflicht.

Externe Entwickler, Contractors, Offshore-Teams und KI-Coding-Agenten erbringen einen wachsenden Anteil der Unternehmenssoftware. Die meisten Organisationen haben keine kontinuierliche Sichtbarkeit darüber, wer ihr wertvollstes geistiges Eigentum einsehen, verändern, kopieren oder offenlegen kann — und europaweit wird genau diese Lücke zur Rechtspflicht auf Vorstandsebene.

VORSTANDSPFLICHT	GESCHÄFTSGEHEIMNISSE	VORSTANDSAUFSICHT	WERT IM RISIKO
§ 93 AktG	**EU 2016/943**	**NIS2**	**€100M+**
Sorgfaltspflicht zum Schutz des Unternehmensvermögens	Schutz nur bei „angemessenen Geheimhaltungsmaßnahmen“	Persönliche Haftung für Cyber-Governance	Unternehmenswert, gebunden an Software-IP

Nach § 93 AktG und vergleichbarem EU-Gesellschaftsrecht können Vorstände persönlich haften, wenn sie wesentliche Unternehmenswerte nicht schützen — zunehmend Software, Algorithmen, KI-Modelle und Geschäftsgeheimnisse.

EXECUTIVE SUMMARY

IP-Schutz ist jetzt Vorstandspflicht

Jahrelang wurden drei Risiken als getrennte Probleme behandelt: **IP-Diebstahl** war ein Rechtsthema, **Cybersecurity** ein IT-Thema und **externe Entwickler** ein Procurement-Thema. Heute konvergieren sie. Unter NIS2, der EU-Geschäftsgeheimnisrichtlinie, nationalem Gesellschaftsrecht und dem kommenden Cyber Resilience Act wird von Vorständen zunehmend erwartet, Aufsicht über Software-Assets, geistiges Eigentum, externe Entwickler, KI-Coding-Agenten und Software-Lieferkettenrisiken nachzuweisen.

Das verschiebt die Diskussion von einem Security-Thema zu einem **Governance-, Compliance- und Haftungsthema** — und wirft eine Frage auf, die die meisten IP-Kontrollen nicht beantworten können: **Können Sie nachweisen, wer die Software einsehen, verändern, kopieren oder offenlegen kann, die Ihr Unternehmen differenziert?**

DER RECHTLICHE WANDEL IN EUROPA

Von drei getrennten Problemen zu einer Vorstandspflicht

HISTORISCH — GETRENNTE SILOS

- IP-Diebstahl = ein Rechtsthema
- Cybersecurity = ein IT-Thema
- Externe Entwickler = Procurement

→

HEUTE — KONVERGIERT AUF VORSTANDSEBENE

Vorstände haben die Pflicht, wesentliche Unternehmenswerte zu schützen.

› Software, Algorithmen, KI-Modelle & Geschäftsgeheimnisse zählen heute zu den wertvollsten.

WAS AUF DEM SPIEL STEHT

Das Risiko — und die Rechtspflicht, die es heute begründet

ZENTRALE IP-RISIKEN MIT EXTERNEN ENTWICKLERN & KI-AGENTEN

Quellcode-Abfluss

Code vor dem Austritt kopiert, andernorts wiederverwendet — oder beim Wettbewerber.

Unbefugter Zugriff

Schlafende Konten, Contractor-Zugriff nach Projektende, geteilte Credentials.

Unsichere Tools & Umgebungen

Nicht freigegebene Tools und Cloud-Dienste schaffen unkontrollierte Abflusskanäle.

IP-Leckage über KI-Tools

Quellcode in KI-Assistenten eingefügt; Prompts legen proprietäre Algorithmen offen.

Eigentumsstreitigkeiten

Unklare Contributor-Ownership, fehlende Autorschaftsnachweise, schwache Governance.

DIE EUROPÄISCHE RECHTSLANDSCHAFT · WARUM VORSTÄNDE HEUTE HAFTEN

§ 93 AktG — Sorgfaltspflicht

DEUTSCHLAND

Vorstände müssen wesentliche Unternehmenswerte schützen — inklusive Quellcode, Algorithmen, KI-Modellen und Geschäftsgeheimnissen.

GeschGehG — Geschäftsgeheimnisse

DEUTSCHLAND

Schutz gilt nur bei „angemessenen Geheimhaltungsmaßnahmen“. Schwache Kontrollen können den Rechtsschutz verwirken.

NIS2-Richtlinie

EU-WEIT

Leitungsorgane müssen Cyber-Risikomaßnahmen billigen, überwachen und verantworten — mit persönlicher Haftung.

Geschäftsgeheimnis-richtlinie

EU 2016/943

Geschäftsgeheimnisse sind nur geschützt, wo das Unternehmen „angemessene Schritte“ zur Geheimhaltung unternommen hat.

Cyber Resilience Act

EU

Secure-by-Design-SDLC und Produkt-Cybersecurity-Verantwortung — wer Code geändert, freigegeben und deployt hat.

Code de Commerce

FRANKREICH

Fiduziarische Direktorenpflichten; die Loi de Vigilance erweitert die Risikoaufsicht über die Lieferanten- & Entwicklerkette.

Burgerlijk Wetboek

NIEDERLANDE

Direktoren müssen das Unternehmen ordnungsgemäß führen; unterlassener Schutz wertvoller Assets kann Haftung begründen.

Codice Civile / LSC

ITALIEN & SPANIEN

Direktoren müssen mit gebotener Sorgfalt den Unternehmenswert erhalten — inklusive Know-how und Quellcode.

TRADITIONELLE IP-SCHUTZ-ANTWORTEN

Wem gehört es — auf dem Papier?

NDA · Vertrag · DLP · Quellcode-Escrow

Definiert Eigentum und Absicht — aber nicht, wer den Code tatsächlich erreichen kann.

BLUEFLAG BEANTWORTET

- ✓ **Welche externen Entwickler haben Zugriff?**
- ✓ **Welche Repositories, Branches & Secrets?**
- ✓ **Welche CI/CD-Pipelines?**
- ✓ **Welche KI-Coding-Agenten?**
- ✓ **Können Sie Governance nachweisen?**

WO BLUEFLAG ANSETZT

Die härteste Frage: Wer kann Ihr IP erreichen?

Traditionelle IP-Kontrollen — NDAs, Verträge, DLP und Escrow — definieren Eigentum auf dem Papier. Sie können nicht zeigen, wer den Code in der Praxis tatsächlich einsehen, verändern, kopieren oder offenlegen kann — über Mitarbeiter, Contractors, Drittentwickler, Maschinenidentitäten und KI-Coding-Agenten hinweg. BlueFlag ist die Governance-, Sichtbarkeits- und Kontrollebene, die es kann.

1 Developer Identity Governance

- Wer hat Zugriff — und auf welche Repositories, Branches und Secrets
- Least Privilege & Just-in-Time-Zugriff
- Starke Authentifizierung & Device Trust
- Kontinuierliche Access Reviews

IP-WERT

„Welche externen Entwickler können unseren Code erreichen?“ — kontinuierlich beantwortet.

2 Code & Data Protection

- Sichere Repositories mit granularen Berechtigungen
- Data-Loss-Prevention auf Code-Bewegungen
- Verschlüsselung in Transit und at Rest

IP-WERT

Ungewöhnliche Code-Bewegungen erkennen, bevor IP die Organisation verlässt.

3 Kontrollierte Dev-Umgebungen

- Isolierte, ephemere Umgebungen
- Keine lokale Code-Speicherung
- Copy / Paste / Download / Screenshots unterbinden

IP-WERT

Contractors entwickeln, ohne dass Code je eine governete Grenze verlässt.

4 Third-Party- & Tool-Security

- Dritt-Tools prüfen und überwachen
- Nicht freigegebene Dienste einschränken
- Integrationen und APIs absichern

IP-WERT

Die unkontrollierten Kanäle schließen, über die IP still abfließt.

5 IP in KI & Automatisierung

- Welche KI-Tools im Einsatz sind — Claude Code, Cursor & andere
- Sensiblen Code von KI-Tools fernhalten
- KI-Tool-Nutzung überwachen und auditieren

IP-WERT

„Wer hat welchen KI-Agenten verbunden — und was hat er berührt?“ — beantwortbar.

6 Governance & Compliance

- Klare IP-Ownership-Definitionen & starke Klauseln
- Audit-Trails und Compliance-Reporting
- Nachweisbare Funktionstrennung

IP-WERT

Die „angemessenen Schritte“ nachweisen, die der Geheimnisschutz heute verlangt.

VOLLSTÄNDIGE SICHTBARKEIT ÜBER DIE ZUGRIFFSKETTE

Entwickler › **Repository** › **Branch & Secret** › **CI/CD-Pipeline** › **KI-Agent**

MAPPING: VORSTANDS- / RECHTSFRAGE → BLUEFLAG-EVIDENZ

PFLICHT	WAS VORSTÄNDE / AUDITOREN / KÄUFER FRAGEN	BLUEFLAG-EVIDENZ
Geschäftsgeheimnis-schutz	Haben wir „angemessene Schritte“ zur Geheimhaltung unternommen?	Zugriffs-Governance, Berechtigungs-Reviews und der Nachweis, dass Zugriffe nach Projektende entzogen wurden.
Vorstandspflicht	Sind unsere wertvollsten Software-Assets governed?	Attribuierbares Inventar jedes Entwicklers, jeder Maschinenidentität und jedes KI-Agenten im SDLC.
Externes-Entwickler-Risiko	Wer kann unseren Code einsehen, verändern oder kopieren?	Identitätskorrelierte Sicht über Source Control, Repositories, Secrets und Pipelines.
KI-Governance	Ist die Nutzung von KI-Coding-Tools kontrolliert?	KI-Agenten-Inventar, KI-Identitäts-Tracking und Code-zu-KI-Exposure-Monitoring.
M&A- / PE-Due-Diligence	Können wir nachweisen, dass unser IP angemessen geschützt ist?	Exportierbare IP-Governance-Evidenz und eine Pre-Acquisition-Readiness-Sicht.

WIE BLUEFLAG FUNKTIONIERT

Connect, Discover, Detect, Remediate — kein Agent, keine Code-Änderungen

1

CONNECT

Vorgefertigte API-Integrationen über Source Control, CI/CD, IAM, Registry und SIEM. In unter 30 Minuten deployt — kein Agent, keine Code-Änderungen.

2

DISCOVER

Kontinuierliches Inventar jedes Entwicklers — Mensch, Non-Human und KI-Agent — und jeder Dev-Tool-Aktivität in einem Identity Graph mit Verhaltens-Baselines.

3

DETECT

Exzessive Berechtigungen, schlafende Contractor-Konten, Zugriff nach Vertragsende, Privilegien-Eskalation und ungewöhnliche Code-Bewegungen sichtbar machen — mit vollem Identitätskontext.

4

REMEDIATE

Policy in Echtzeit durchsetzen — Zugriffe richtig dimensionieren, KI-Tool-Nutzung governen und audit-fertige Evidenz für IP-Schutz erzeugen.

DER BUSINESS VALUE

Die Assets schützen, die das Unternehmen differenzieren

Proprietären Code & Algorithmen schützen

Trading-Algorithmen, Steuerungssoftware, KI-Modelle und Roadmaps, die den Kernwert des Unternehmens ausmachen.

Wettbewerbsvorteil erhalten

Die differenzierende Software im Unternehmen halten — governed über Menschen, Maschinen und KI.

IP-Diebstahl & Rechtsrisiko senken

Die „angemessenen Schritte" des Geheimnisschutzrechts nachweisen und die Haftungsexposition des Vorstands reduzieren.

Unternehmens- & M&A-Wert bewahren

Due-Diligence-fertige Evidenz; ein materieller IP-Leckage-Vorfall wirkt direkt auf die Bewertung.

WARUM C-SUITE & VORSTAND PROFITIEREN

CISO / CSO	Ein vor dem Vorstand vertretbares, attribuierbares Inventar jedes Entwicklers, Contractors, jeder Maschinenidentität und jedes KI-Agenten mit Zugriff auf Quellcode — mit Policy-Durchsetzung in Echtzeit, nicht als Absichtserklärung.
CIO / CTO	Externe und KI-getriebene Entwicklung sicher und skalierbar operationalisieren — governen, wer und was auf den Code zugreifen kann, ohne Engineering auszubremsen.
CFO	Die Software-Assets schützen, die hunderte Millionen Euro Unternehmenswert tragen — und die Breach-, Haftungs- und Bewertungsexposition eines IP-Verlusts reduzieren.
General Counsel / GRC	Die „angemessenen Schritte" und die Funktionstrennung nach Geschäftsgeheimnisrichtlinie, § 93 AktG, NIS2 und CRA nachweisen — mit exportierbarer Evidenz.
Vorstand / PE-Investor	Die Haftungsfrage direkt beantworten: Können wir nachweisen, dass unsere wertvollsten Software-Assets angemessen geschützt sind — vor und nach der Akquisition?

EXECUTIVE MESSAGE

„Nach § 93 AktG und vergleichbarem EU-Gesellschaftsrecht haben Vorstände die Pflicht, die wertvollsten Assets des Unternehmens zu schützen. Heute sind diese Assets Software, Algorithmen, KI-Modelle und Geschäftsgeheimnisse. BlueFlag Security liefert kontinuierliche Sichtbarkeit und Governance darüber, wer sie einsehen, verändern, kopieren oder offenlegen kann — über Mitarbeiter, Contractors, Drittentwickler, Maschinenidentitäten und KI-Coding-Agenten hinweg."

Raj Mallempati · CEO & Founder, BlueFlag Security